#8

| TRANSMITTAL LETTER (General - Patent Pending) | Docket No. 112857-075 |
|---|---|

In Re Application Of: **Haruo Oba et al.**



| Serial No. | Filing Date | Examiner | Group Art Unit |
|---|---|---|---|
| 09/696,927 | October 26, 2000 | | |

Title: **AUTHENTICATION INFORMATION COMMUNICATION SYSTEM AND METHOD, PORTABLE INFORMATION PROCESSING DEVICE AND PROGRLAM FURNISHING MEDIUM**



TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Transmitted herewith is:

**Certified copy of Japanese Priority Document Noumbers 11-310517 and 2000-253305**

in the above identified application.

- ☒ No additional fee is required.
- ☐ A check in the amount of is attached.
- ☒ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. **02-1818** as described below. A duplicate copy of this sheet is enclosed.
  - ☐ Charge the amount of
  - ☐ Credit any overpayment.
  - ☒ Charge any additional fee required.

*Signature*

Dated: **October 9, 2001**

**William E. Vaughan (Reg. No. 39,056)**
**Bell, Boyd & Lloyd LLC**
**P.O. Box 1135**
**Chicago, Illinois 60690**

I certify that this document and fee is being deposited on **October 9, 2001** with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

*Signature of Person Mailing Correspondence*

**Robert Buccieri**

*Typed or Printed Name of Person Mailing Correspondence*

cc:

# 日本国特許庁
# PATENT OFFICE
# JAPANESE GOVERNMENT

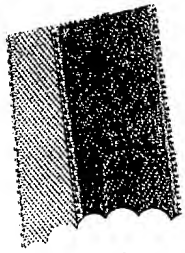
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

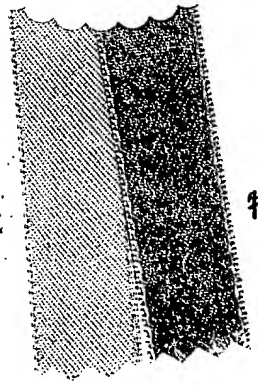
出願年月日
Date of Application: １９９９年１１月　１日

出願番号
Application Number: 平成１１年特許願第３１０５１７号

出願人
Applicant (s): ソニー株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年　９月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０７３６００

【書類名】　特許願

【整理番号】　99007026

【提出日】　平成11年11月 1日

【あて先】　特許庁長官殿

【国際特許分類】　G06K 17/00

【発明の名称】　認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【請求項の数】　24

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　大場　晴夫

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　戸塚　恵一

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　沼岡　千里

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点Ｂと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段と、

を有することを特徴とする認証情報通信システム。

【請求項２】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項３】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認

証用データに基づく認証処理を実行する認証手段を有し、

前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項４】

前記サービス提供装置は、

提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を有し、

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、

前記サービス提供装置から前記接点Ｂおよび前記接点Ａを介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項５】

前記サービス提供装置は、

提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項６】

前記認証情報通信システムは、さらに、

ユーザに対する認証処理を実行するユーザ管理手段を有し、

前記ユーザ管理手段は、

ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有すること

を特徴とする請求項１に記載の認証情報通信システム。

【請求項７】

前記認証情報通信システムは、さらに、

ユーザに対する提供サービスを登録するサービス登録手段を有し、

該サービス登録手段は、

前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項８】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項１に記載の認証情報通信システム。

【請求項９】

サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置。

【請求項１０】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づ

く認証用データを生成する構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１１】

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、

前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１２】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１３】

前記接点Ａは、人体の装着部に沿った曲線形状を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１４】

前記携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１５】

前記携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１６】

前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１７】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装

置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点Ｂおよび接点Ａを介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点Ａおよび接点Ｂを介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする認証情報通信方法。

【請求項１８】

前記認証用データ生成ステップは、

前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする請求項１７に記載の認証情報通信方法。

【請求項１９】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、

前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２０】

前記認証情報通信方法において、

前記サービス提供装置は、

さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２１】

前記認証情報通信方法において、さらに、

ユーザに対する認証処理を実行するユーザ管理ステップを有し、

前記ユーザ管理ステップは、

ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、

前記認証処理は、該登録テーブルに基づいて実行することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２２】

前記認証情報通信方法において、さらに、

ユーザに対する提供サービスを登録するサービス登録ステップを有し、

該サービス登録ステップは、

前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、

前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２３】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記接点Ｂを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Ｂを介して受信するステップと

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とするプログラム提供媒体。

【請求項２４】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、携帯情報処理装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記携帯情報処理装置に対して出力されるサービス識別データを前記接点Ａを介して受信するステップと、

前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記サービス提供装置に対して、前記接点Ａを介して前記認証用データを出力するステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体に関する。さらに詳細には、外部機器に設けた電極である接点に人体の一部、例えば手が接触することによって、人体に装着したや

はり電極としての接点を設けた携帯機器とのデータ通信を可能とし、個人認証に必要なデータを人体を介して転送して個人認証処理、および外部機器との情報交換を可能にした個人認証情報通信システムおよび個人認証情報通信方法に関する構成を開示するものである。本発明に適用される携帯機器は、例えば時計や指輪のように曲線状の形状を有する取付具部を有し、人が通常身につける小型の物品において実現され、これらの装身具に個人認証のためのデータを記憶する構成としたものである。

【０００２】

【従来の技術】

従来、非接触型カード等を利用して個人認証を行い、認証の可否に基づいて外部装置を制御するシステムは良く知られている（例えば特開平１１－１６１７６３など）。非接触型カードは、定期券、プリペイドカード等の接触型カードに変わるシステムとして今後有効な手法として期待される構成の一つである。

【０００３】

しかしながら、このような非接触型カードを使用するユーザは、カードによる認証を受ける場合、カード自体を手に取り、例えばセンサ等の情報読み取り装置に取りだしたカードを近づけて読み取り処理を実行させる必要があり、これらの各処理に時間を要するという欠点がある。例えば入場ゲート、改札を通過するときなどの限られた時間内に一連の処理を次々と実行させなければならない場合、個人認証のためのカード読み取り、読み取りデータに基づく認証処理、認証処理に基づく改札ゲートの開閉動作を複数のユーザに対して次々と実行する必要があり、１人あたりの処理時間の増加は多人数の処理においてさらに大きな処理時間の増加をもたらし、実用化を困難にする原因となっている。この意味で非接触型カードは従来の接触型カードに比較して、すべての面で優れているとは言い難い。

【０００４】

さらに、非接触型カードまたはカード型以外の認証用携帯機器を使用するユーザは、ユーザが取り出した、または身につけたカード等の認証機器を認証装置あるいは処理装置に近づける、あるいは近くを通りすぎる等、きわめて曖昧な処理

を実行することが要求され、認証装置あるいは処理装置に直接触れるという処理を伴わないので、実際にデータの読み取りに成功しているのか、または個人認証処理が実行されているのか等の実感が得られず、処理の開始タイミング等が全くユーザには判別できない。従って、処理が遂行されているか否かの判定が曖昧になってしまい、結果として、所定時間後に例えばゲートが開かないといったエラーが生じ、このエラーが生じるまでは、読み取り処理の失敗、または認証されなかったという結果が得られないという欠点がある。

【０００５】

本発明の個人認証情報通信システムおよび個人認証情報通信方法は、係る状況に鑑み、従来の接触型カード、非接触型カードと同様に個人認証を実行して各種の処理を実行させるシステムおよび方法において、個人認証を行なおうとするユーザが認証システムを構成する装置に形成された接点に対して人体の一部、例えば指、または手のひら等を接触させることで人体を介して個人認証用データ転送を行ない、ユーザの個人認証処理の開始をユーザ自身が認識することを可能とし、個人認証処理システムの使い勝手を改善するとともに、ユーザに対して認証処理及び認証処理に基づく各種処理の実行が開始されたことの達成感を与えることができるシステムを提供するものである。

【０００６】

上述のような人体を介してデータ転送を行なうシステムを開示した従来例としては、例えば以下に示すものがある。

【０００７】

特開平７－１７０２１５、ＵＳＰ５，９１４，７０１には、電極を有する２つの互いに独立なシステムにおいて、そのままでは互いに通信するには不充分な程度の微弱電波をシステム間で発信し、そのシステム間に人体が介在することにより、人体を媒介としてシステム間のデータ転送を実行する構成が開示されている。例えば特開平７－１７０２１５では、オーディオ／ビデオ信号等を導電性部材と人体を介して転送し、ディスプレイ、スピーカを備えた受信端末に出力する構成が記載されている。

【０００８】

また、ＵＳＰ５，７９６，８２７では、人体を介したデータ転送を使用したシステムにおいて、さらに暗号化したデータを送受する手段を加えることによって、クレジットカードあるいはキャッシュカードなどに応用するというアイデアを開示している。具体的には、送信機から受信機に対する符号化データの転送を人体を伝送媒体として実行し、受信機に接続された認証処理装置が人体を介して送られた符号化データを処理して認証を行なう構成である。当ＵＳＰ５，７９６，８２７では、人体を介するデータ転送を実行するための電極をユーザが日常、身につける物品に組み込み可能とした構成が示され、その例として腕時計、衣服、または靴が記載されている。このような日常的に体に接触している物品、いわゆる装身具に電極を組み込むことにより、ユーザが専用の電極構成体を新たに装着することを不要としている。

【０００９】

【発明が解決しようとする課題】

しかしながら、昨今サービスの種類は多様化し、認証処理を行なった後に実行すべき処理の態様は、ユーザによっても、また場所、時間によっても異なるものとすることが好ましい場合が多い。ユーザを認証処理によって識別して一律に認証の可否に応じた処理を実行することは、提供されるサービスの内容が固定的になり好ましくない。例えば、情報提供サービスを実行するサービス提供端末において、ＢＧＭ提供を受けようとすると、ユーザＡは、クラシックが好みであり、ユーザＢはロックが好みである場合、単なる認証処理に基づいて、同一の音楽配信をすると好みと無関係な音楽情報が配信される。あるいはサービス提供端末が遊園地のゲートの開閉処理を制御する端末である場合、ユーザ毎にゲート開閉の有効時間、有効場所を設定することが望ましい。

【００１０】

もちろん、ユーザ毎に提供サービスを設定するテーブルを設け、ユーザＩＤに基づいて提供サービスを決定し、決定したサービスを実行することも可能であるが、これらのデータ処理、すなわち情報提供端末からの中央処理装置へのデータ転送、データ処理装置におけるデータ処理、処理態様決定、さらに情報提供装置へのデータ転送等に時間を要し、次々に異なるユーザに対する処理を実行しなけ

ればならない環境等においては、処理時間の遅延が蓄積してしまうことになる。

【００１１】

係る事情に鑑み、本発明は、ユーザ毎、サービス毎に異なる態様での処理を即座に実行可能にするように、各サービス毎に独立であり、かつ各ユーザ毎にユニークである認証用データを作成し、これをユーザの携帯機器に格納し、サービスの要求時にこの認証用データを出力できるようにしたものである。

【００１２】

さらに本発明は、非接触型カードが持つ利便性を損なうことなく、ユーザがサービス提供端末の接点に触れることによってユーザに処理の達成感を与えることができるように、人体を介して通信を行う携帯情報処理装置の接点を人体に接触した状態で装着するため、曲線状の接点部を持つ構成としたものである。

【００１３】

【課題を解決するための手段】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、

人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点Ｂと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段と、を有することを特徴とする認証情報通信システムにある。

【００１４】

さらに、本発明の認証情報通信システムにおいて、前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする。

【００１５】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証手段を有し、前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする。

【００１６】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を有し、前記携帯情報処理装置は、前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、前記サービス提供装置から前記接点Ｂおよび前記接点Ａを介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【００１７】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【００１８】

さらに、本発明の認証情報通信システムは、さらに、ユーザに対する認証処理を実行するユーザ管理手段を有し、前記ユーザ管理手段は、ユーザ登録状況およ

び、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有することを特徴とする。

【００１９】

さらに、本発明の認証情報通信システムは、さらに、ユーザに対する提供サービスを登録するサービス登録手段を有し、該サービス登録手段は、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【００２０】

さらに、本発明の認証情報通信システムにおいて、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする。

【００２１】

さらに、本発明の第２の側面は、

サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置にある。

【００２２】

さらに、本発明の携帯情報処理装置は、前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを

特徴とする。

【００２３】

さらに、本発明の携帯情報処理装置は、前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【００２４】

さらに、本発明の携帯情報処理装置において、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする。

【００２５】

さらに、本発明の携帯情報処理装置において、前記接点Ａは、人体の装着部に沿った曲線形状を有することを特徴とする。

【００２６】

さらに、本発明の携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする。

【００２７】

さらに、本発明の携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする。

【００２８】

さらに、本発明の携帯情報処理装置において、前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする。

【００２９】

さらに、本発明の第３の側面は、

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点Ｂおよび接点Ａを介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点Ａおよび接点Ｂを介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする認証情報通信方法にある。

【００３０】

さらに、本発明の認証情報通信方法において、前記認証用データ生成ステップは、前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする。

【００３１】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする。

【００３２】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする。

【００３３】

さらに、本発明の認証情報通信方法において、前記認証情報通信方法において、さらに、

ユーザに対する認証処理を実行するユーザ管理ステップを有し、前記ユーザ管理ステップは、ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、前記認証処理は、該登録テーブルに基づいて実行することを特徴とする。

【００３４】

さらに、本発明の認証情報通信方法において、さらに、ユーザに対する提供サービスを登録するサービス登録ステップを有し、該サービス登録ステップは、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを特徴とする。

【００３５】

さらに、本発明の第４の側面は、

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記接点Ｂを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Ｂを介して受信するステップと

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とするプログラム提供媒体にある。

【００３６】

さらに、本発明の第５の側面は、

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、携帯情報処理装置で実行する処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

前記サービス提供装置から前記携帯情報処理装置に対して出力されるサービス識別データを前記接点Ａを介して受信するステップと、

前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記サービス提供装置に対して、前記接点Ａを介して前記認証用データを出力するステップと、

を有することを特徴とするプログラム提供媒体にある。

【００３７】

本発明の第４および第５の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３８】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され

、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３９】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４０】

【発明の実施の形態】

以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【００４１】

［実施例１］

本発明の認証情報通信システムの実施例１を構成する送受信装置全体の基本構成を示すブロック図として図１に示す。

【００４２】

図１に示すように、本発明の認証情報通信システムは、携帯機器１０と、サービス端末２０を基本構成とし、携帯機器１０とサービス端末２０間でのデータ転送を人体を介して実行するものである。携帯機器１０は、ユーザ３０が保持または装着可能な機器として構成され、例えば腕時計、ネックレス、ブレスレット、指輪等の装身具、またはカード等の部材によって構成することができ、接点１８は人体、すなわちユーザ３０と接触あるいは導通可能に極めて近接した状態に設定される。

【００４３】

サービス端末２０は、例えば、街頭あるいは店内などに配置されている音楽情報、映像情報、地図情報、その他、各種の情報提供あるいは商品販売用端末、あるいは銀行に設置されたＡＴＭ端末、交通機関としての駅の改札ゲート、飛行機、電車その他の公共的乗り物の座席、あるいは建築物の壁に埋設して設置されているような、様々なサービスを提供する装置である。ユーザ３０がサービス端末２０の接点２９に接触、すなわち指を触れたり、手のひらで触れたりすることにより、携帯機器１０とサービス端末２０の間で通信が可能になる。

【００４４】

人体を介する携帯機器１０と、サービス端末２０間のデータ転送は、携帯機器

１０に形成された接点１８と、サービス端末２０に形成された接点２９の両接点に同時に人体、すなわちユーザ３０の一部が接触することによって実行される。なお、携帯機器１０は例えば腕時計等の装身具であるので、接点１８は、基本的に常時人体に接触、あるいは導通可能に極めて近接した状態となっている。従って、ユーザ３０がサービス端末２０の接点２９に触れた時点で、人体を介する携帯機器１０とサービス端末２０間のデータ転送が実行可能となる。

【００４５】

携帯機器１０とサービス端末２０間のデータ転送は、携帯機器１０の通信部１５と、サービス端末２０の通信部２５との間で実行される。この人体を介した通信は、例えば、特開平７－１７０２１５に記載の構成が適用できる。人体は、そのほとんどを塩分を含んだ水からなる導電性の容器と考えられるので、数ＭＨｚ帯では概ね導体となる。なお、テスター等で両手間の直流抵抗を計測すると、手の状態に応じて５００ｋΩから２，３ＭΩの値を示す。

【００４６】

人体の交流における伝達特性を図２に示す。図２（ａ）は１ＭＨｚ～２０ＭＨｚ、図２（ｂ）は１ＭＨｚ～３０ＭＨｚの範囲で、スペクトラムアナライザを用いて測定した人体の伝送特性（両手間）を示す特性図である。いずれも、トラッキングジェネレータと入力端子に同軸ケーブルを接続した場合の例である。なお、同軸ケーブルのグランドＧＮＤは相互に接続し、アンテナとならないようにした。図２（ａ）および（ｂ）に示すように、１ＭＨｚから２０ＭＨｚ程度の範囲における伝達特性は、概ね平坦で３０ｄＢないし４０ｄＢの減衰特性となる。

【００４７】

図２（ａ）および（ｂ）に示す測定では、トラッキングジェネレータの出力インピーダンス、スペクトルアナライザの入力インピーダンスとも７５Ωである。したがって、もし、交流的にも両手間のインピーダンスが、例えば１メガオームであったとすると、減衰量は－８０ｄＢにも達する筈である。ところが、実際には、減衰量は遥かに少なく、人体を介しての信号伝送の可能性を裏付けることが分る。

【００４８】

データ送信側は、微小ダイポールアンテナと考えられ、これが発生する電磁界の様子は十分解析されている。それによれば、人体が発生する電磁界は、微小ダイポールアンテナが発生する電磁界となる。電磁界の強さはアンテナからの距離Ｒ、距離Ｒの２乗、距離Ｒの３乗に反比例する成分のベクトル和で表され、それぞれ、輻射電磁界、誘導電磁界、静電磁界と呼ばれる。なお、これらの関係式については、特開平７－１７０２１５号に詳しく記載されている。

【００４９】

図３は電界強度についての図であり、図３（ａ）は、上述した各項の電界強度とアンテナからの距離との関係を示す特性図である。また、図３（ｂ）は、周波数ｆ＝２００ＭＨｚ、送信端子電圧＝１００ｄＢμＶ（７５Ω）の場合において、λ／２．２のダイポールアンテナと３．４ｃｍφのループアンテナ、および８ｃｍφ，３．４ｃｍφのループアンテナの電界強度と距離とを示す図である。図３（ａ）および（ｂ）に示すように、上記輻射電磁界（１／Ｒ項）、誘導電磁界（１／（Ｒの２乗）項）、静電磁界（１／（Ｒの３乗）項）の強度は、λ／２πの距離において等しくなり、距離がこれ以下の場合には急激に増加する。ｆ＝１１ＭＨｚならば、この距離は約４．３ｍとなる。本発明の認証情報通信システムでは静電磁界を主として使用した伝送方式を適用することが好ましい。

【００５０】

また、電解強度は、また電波法のＥＭＩ（Ｅｌｅｃｔｒｏｍａｇｎｅｔｉｃ ｉｎｔｅｒｆｅｒｅｎｃｅ）規制による制限なく使用可能な範囲を選択することが好ましく、例えば、周波数３３２ＭＨｚ以下、電解強度５００μＶ／Ｍ以下とする。

【００５１】

上述のように静電磁界は距離Ｒの３乗で減衰する。例えば、距離が１ｍから３ｍになると、電界強度は１／２７（１／（３×３×３））になる。従って、データ送信手段からの距離が増加すると、信号強度が極端に減衰するので、複数のユーザが同様の装置を使用している場合であっても他のユーザの信号をノイズとしてとらえる可能性は低くなり、例えば同様の装置を持ったユーザが多数近接して存在する環境下においても、静電磁界を主として使用した通信は良好な通信が可

能になる。

【００５２】

なお、携帯機器１０に構成される接点１８は、広い面積を有することが望ましく、例えば腕時計、ネックレス、指輪、ブレスレット等、曲線状に人体の指、腕、首等に巻き付け可能な構成として、人体の皮膚とより多くの面積で接触する構成とすることが好ましい。

【００５３】

携帯機器１０は、クレジットカードの認証番号、ＡＴＭの暗証番号などのように、個人認証の目的で利用されるＩＤを記憶する認証用データ記憶部としての固定データ記憶部１６、可変データ記憶部１７を有している。固定データ記憶部１６にはユーザ固有の固定ユーザ識別子が格納される。可変データ記憶部１７には、例えば、サービス端末のサービスに応じた識別子等、可変ユーザ識別子が格納される。これらの識別子の態様、および処理については後段で詳細に説明する。なお、固定データ記憶部１６と可変データ記憶部１７は携帯機器１０に対して着脱可能なメモリとして構成してもよい。

【００５４】

これらの固定ユーザ識別子、可変ユーザ識別子、あるいはこれらに基づく識別情報が携帯機器１０の通信部１５からサービス端末２０の通信部２５に送付されることによって、サービス端末２０のＣＰＵ２１において認証チェックがなされ、サービス端末２０の例えばＲＡＭ２２などに記憶された情報にアクセスすることができ、サービス端末２０は、ＲＡＭ格納情報をサービス端末２０の通信部２５から携帯機器１０の通信部１５に送付し、データを受信した携帯機器１０は、ＲＡＭ１２等の記憶回路に受信データを蓄えることができる。なお、携帯機器１０のＲＯＭ１３やサービス端末２０のＲＯＭ２３には、それぞれの装置の基本的な制御を行うＯＳやデバイスドライバなどの基本ソフトウェアが記憶されており、電源を入れることによってＣＰＵによって読み出されそれぞれの装置を機能させることができる。

【００５５】

携帯機器１０の電源としては、図示していないが長寿命かつ小型の電源を使用

することが望ましく、例えばリチウム電池バッテリを使用することができる。ＣＰＵ１１は、リチウム電池バッテリからの電源供給を受けてデータの読み出し、データ送信、データ受信、データ蓄積等の各種処理制御を実行する。

【００５６】

携帯機器１０とサービス端末２０との間での通信は、例えばサービス端末２０の接点２９に人体、すなわちユーザ３０の一部が触れたことをサービス端末２０に設けた検知手段が検出し、この検出に応じて、サービス端末２０から後述するサービス識別子を通信部２５、接点２９、ユーザ３０を介して携帯機器１０に出力することにより開始することが可能である。

【００５７】

あるいは、サービス端末２０の通信部２５が連続的に、または数秒毎に、サービス識別子格納手段２８に格納されたサービス識別子データを出力する構成としてもよい。この構成における通信部２５のデータ出力間隔は、ユーザ３０がサービス端末２０の接点２９に指等を触れる数秒間に少なくとも１回は、送信信号がユーザを介してユーザの携帯する携帯端末１０の通信部１５によって受信されるような間隔とする。

【００５８】

あるいは、上記とは逆に、携帯機器１０の通信部１５が連続的に、または数秒毎に、固定データ記憶部１６、または可変データ記憶部１７に記憶されたユーザＩＤなどの信号を送信する構成としてもよい。この場合もユーザ３０がサービス端末２０の接点２９に指等を触れる数秒間に少なくとも１回は、送信信号がサービス端末２０の通信部２５によって受信されるような間隔で発生する構成とする。

【００５９】

送信信号の種類は、後述するように認証処理においては、例えば、ユーザＩＤ、サービス識別子等の認証のために必要なデータである。

【００６０】

認証処理後においては、サービス提供端末において、認証に基づく様々な処理が実行される。例えば改札ゲートの開閉処理、ＡＴＭの入出金処理、あるいは音

楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供処理等である。

【００６１】

なお、音楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供を人体を介して転送して携帯機器に蓄積、あるいは付属のディスプレイ等の出力手段で出力する構成としてもよい。なお転送データ中に秘密情報を含む場合は、送信データは、データ送信側で暗号化して、受信側で復号する構成とすることが好ましい。この場合、データ送信側には、例えば、乱数発生手段、タイムスタンプ処理手段等、各種暗号化処理手段を構成する。一方、受信側には、受信した暗号化データを復号する復号手段を構成する。

【００６２】

携帯機器１０とサービス端末２０に構成される通信部は、ユーザ３０と各接点１８，２９との物理的接触により、信号を送受信する。受信信号は各通信部に構成された復調器により復調され、ＣＰＵ２１の制御のもとに、各端末内の回線、あるいは端末外のネットワークを通じて、各記憶手段、情報処理手段、あるいは認証処理手段等に転送される。

【００６３】

なお、携帯機器１０は、データ送信、データ処理が必要な場合にのみ、ＣＰＵに対する電源供給を実行するように構成してもよい。例えば、サービス端末２０からの受信信号に基づいて電源供給を開始する構成とすれば、携帯機器１０のバッテリ寿命を延ばすことができる。

【００６４】

以下、図１に示す認証情報通信システムにおける認証処理、およびデータ転送処理を具体例を示しながら説明する。携帯端末１０を装着したユーザ３０がサービス端末２０に接点２９で接触したとする。ユーザ３０がはじめてサービス端末２０に接触した場合には、認証のための登録処理がなされる。

【００６５】

認証登録処理のためにサービス端末２０では認証用ユーザ識別子生成部２６において認証用のユーザ識別データ（可変ユーザ識別子）を生成し、このユーザ識

別データ（可変ユーザ識別子）をサービス識別子２８と共に、通信部２５を経由して携帯端末１０の通信部１５に対して送信する。送信されたユーザ識別データ（可変ユーザ識別子）は、携帯端末１０の可変データ記憶部１７に記憶される。

【００６６】

可変データ記憶部１７の構成および合成部１４での処理を説明する図を図４に示す。可変データ記憶部１７は、例えば図４に示すようにテーブル構造をなしており、サービス端末２０から受信したサービス識別子（例えばサービスＩＤ：１０１）をキーとするレコードに対して、認証用ユーザ識別子（可変ユーザＩＤ：００００１００１１）を格納する構成となっている。

【００６７】

携帯機器１０の合成部１４は、図４に示すようにサービス端末２０から受信した認証用ユーザ識別子（可変ユーザ識別子（ＩＤ）：００００１００１１）と、予め固定データ記憶部１６に格納されているユーザ固有の固定識別子（固定ユーザ識別子（ＩＤ）：１０１００００００）との合成処理を実行する。

【００６８】

合成部１４における合成処理により生成された識別子は、そのユーザ（固定ユーザＩＤ：１０１００００００によって特定される）にのみ有効であり、さらにそのサービス（例えばサービスＩＤ：１０１によって規定されるサービス）にのみ有効な識別子、すなわち特定サービスに有効なサービス固有のユーザ識別子である。

【００６９】

携帯機器１０は、この合成部１４において生成された特定サービスに有効なサービス固有のユーザ識別子、例えば図４右上に記載のサービス：０１０用のユーザ識別子（ＩＤ）「１０１００００００／００００１００１１」を、サービス端末２０に対して送信する。携帯機器１０からサービス端末２０に対して人体を介して送信されるこのサービス固有のユーザ識別子は携帯機器１０の接点１８、ユーザ３０、サービス端末２０の接点２９を通じてサービス端末２０の通信部２５において受信される。

【００７０】

サービス端末２０は受信データを、認証用データ記憶部２７に記憶する。認証用データ記憶部２７は、可変データ記憶部１７と同様の例えばハッシュテーブル構造、すなわち認証用ユーザ識別子としての固定ユーザ識別子をキーとしたテーブル構成を有しており、受信したサービス固有のユーザ識別子をテーブルに記憶する。

【００７１】

ユーザ３０がサービス端末２０に接触したのが初めてでない場合には、サービス端末２０が保持するサービス識別子２８のデータ（例えば０１０）を受信した携帯端末１０は、受信サービス識別子に基づいて可変データ記憶部１７から受信したサービス識別子に対応する認証用ユーザ識別子（可変ユーザＩＤ）を取り出して、合成部１４において、固定データ記憶部１６に格納されているユーザ固有の固定識別子（固定ユーザＩＤ）との合成処理を実行してサービス固有のユーザ識別子を生成してサービス端末２０に送信する。

【００７２】

図４を用いてこの処理の具体例について説明する。サービス端末２０の提供するサービス識別子が「０１０」であったとする。例えばサービス端末２０がコンビニに設置された情報提供端末であり、サービス識別子が「０１０」が商品割引券発行サービスであるとする。携帯端末１０（例えば腕時計に内蔵されている）を有するユーザは、コンビニに設置されたサービス端末２０の接点２９に指、あるいは手のひらを触れる。サービス端末２０は、接点２９に設置されたセンサにより、指、あるいは手のひらの接触を検出し、ＣＰＵ２１の制御の下にサービス識別子保持部２５からサービス識別子「０１０」を取り出して、これを通信部２５を介してユーザ３０に出力する。サービス識別子「０１０」は、ユーザ３０の人体を介して、ユーザの皮膚と接点１８を持つ腕時計型の携帯端末１０によって受信される。

【００７３】

サービス識別子「０１０」を受信した携帯端末１０は、可変データ記憶部１７を検索して、サービス識別子「０１０」に相当する可変ユーザＩＤとして「０００１００１１」を取り出し、取り出した可変ユーザＩＤ「０００１００１１」を

合成部１４に送る。合成部１４は、可変ユーザＩＤ「００００１００１１」と、固定データ記憶部１６に記憶されている固定ユーザＩＤ「１０１０００００」とを合成し、「１０１０００００００１００１１」という特定サービスに有効なサービス固有のユーザ識別子データを得て、これを通信部１５、接点１８、ユーザ３０の人体、サービス端末２０の接点２９、を介してサービス端末２０の通信部２５に送信する。

【００７４】

上述の処理を経て特定サービスに有効なサービス固有のユーザ識別子データを携帯端末１０から受信したサービス端末２０は、認証処理を行なう。この認証処理について図５を用いて説明する。

【００７５】

サービス端末２０では、携帯端末１０から送信されるサービス固有のユーザ識別子データ、すなわち上述のデータ「１０１０００００００１００１１」を受信すると、認証部２４において、固定ユーザＩＤ「１０１０００００」と、可変ユーザＩＤ「００００１００１１」とに分離する処理を行なう。さらに、認証データ記憶部２７にアクセスして、これらの識別子が認証データ記憶部２７に登録済みのＩＤに対応するか否かの確認、すなわち認証処理を行う。正しくデータ照合がなされた場合、すなわち認証がされた場合には、サービス端末２０に規定されたサービス、すなわち上述のサービス識別子「０１０」に相当するサービス、例えば商品割引券発行サービスを実行する。サービス端末には、商品割引券発行手段が接続、または内蔵され、この商品割引券発行手段が認証処理に基づいて商品割引券発行処理を開始する。

【００７６】

可変ユーザＩＤは、例えばサービス端末２０において商品割引券発行が可能な期間を設定したデータとして構成することができる。この構成とした場合、可変ユーザＩＤを受信したサービス端末２０は、その可変ユーザＩＤから有効期間を判定して、有効期間内の場合にのみ正当なサービスを受けるユーザであると判定し、サービスを実行する。また、定期券等の場合は、期間、区間データも併せて可変ユーザＩＤ中に登録することで、携帯機器から受信した可変ユーザＩＤのみ

からその有効性を判定することが可能となる。

【００７７】

サービス端末２０が提供するサービスは、例えば入場ゲート、改札、建物の入口、研究室ドアの開閉処理であったり、画像、音声データ等の出力処理、ＡＴＭにおける入金、出金処理等、様々なサービスである。サービスが改札ゲートの開閉である場合は、上述の認証処理に基づいて、改札がオープンし、認証されたユーザのみが改札を通ることができる。この場合、サービス端末２０の接点２９は各改札ゲートに設置される。

【００７８】

なお、サービス端末２０は、複数のサービス識別子を保持し、各々のサービス識別子に対応してサービス固有のユーザ識別子データを格納したテーブルを保持する構成とすることにより、各個人に対して異なるサービスを提供することが可能である。

【００７９】

なお、上述の例では、固定ユーザＩＤと可変ユーザＩＤとを単純に連結したデータを合成データとして生成し、これをサービス固有のユーザ識別データとする例を説明したが、サービス固有のユーザ識別データの生成は、上述した方法に限らず、固定ユーザＩＤと可変ユーザＩＤに基づいて予め定めた関数等により新たなデータ列を生成してサービス端末２０に送信し、サービス端末２０がこれを解読する構成としてもよい。これらの関数処理、解読処理は、例えば暗号化処理、復号処理の組合わせとしてもよい。また、可変ユーザＩＤのみをサービス端末２０に出力して、サービス端末２０が可変ユーザＩＤのみに基づいて認証処理を実行してユーザの識別及びサービスの実行可否を決定するように構成してもよい。サービス端末２０は、サービスに応じてユーザに可変ユーザＩＤを設定する構成であるので、可変ユーザＩＤのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になる。

【００８０】

サービス端末２０が情報提供を行なう端末である場合、認証処理に基づいて提供する音楽情報、画像情報等、様々な情報は、サービス端末２０に設けたディス

プレイ等の表示手段に表示してもよく、さらに、携帯機器に付属して設けたディスプレイ等の出力手段に、上述の認証データと同様に人体を介してサービス端末から画像情報等を転送して、ユーザに提供する構成としてもよい。なお、人体を介した画像、音声情報等の伝送態様については、本出願と同一出願人による先の特許出願（特開平７－１７０２１５号）に詳細に説明されている。

【００８１】

携帯端末１０の例を図６に示す。図６（ａ）は、ブレスレット６０１に接点を設けて、内部に図１に示す携帯機器１０としての構成を内蔵したものである。図６（ｂ）は、ネックレス６０２に接点を設けて、内部に図１に示す携帯機器１０としての構成を内蔵したものである。図６（ｃ）は、指輪６０３に接点を設けて、内部に図１に示す携帯機器１０としての構成を内蔵したものである。図６（ｄ）は、腕時計６０４に接点を設けて、内部に図１に示す携帯機器１０としての構成を内蔵したものである。ブレスレット６０１、ネックレス６０２、指輪６０３、および腕時計６０４の接点は、それぞれ人体と接触する側、すなわち内周側に設けられ、各接点を介して、ユーザである人体、さらにユーザの指、手のひら等、図１に示すサービス端末２０の接点２９に触れた人体の物理的接触点を介して携帯機器１０とサービス端末２０との間のデータ転送が可能になる。このように、携帯端末１０は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレット等、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有する。

【００８２】

次に、図７～９を用いて本発明の認証情報通信システムにおける認証処理フローについて説明する。図７は、図１に示す認証情報通信システムにおける携帯機器１０の処理フローであり、図８および図９は、図１に示す認証情報通信システムにおけるサービス端末２０の異なる態様での処理フローを示す。

【００８３】

まず、図７の携帯機器１０の処理フローについて説明する。ステップ７０１はデータ受信のため、接点１８の電位上昇を確認するステップであり、データ受信に必要な電位を閾値として接点１８の電位を判定するステップである。接点電位がデータ受信可能状態になると、ステップ７０２において、サービス端末２０か

らユーザ３０の人体を介して送られるサービスＩＤを受信する。

【００８４】

サービスＩＤを受信した携帯端末１０は、ステップ７０３において、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証用ＩＤを生成し、ステップ７０４において、生成した認証用ＩＤをサービス端末２０に対して人体を介して出力する。

【００８５】

認証用ＩＤをサービス端末２０に出力した携帯端末１０は、ステップ７０５において受信側、すなわちサービス端末からの承認応答を待つ。承認応答を受信した場合は、サービス端末２０からのさらなる処理要求を待機（ステップ７０６）し、要求があった場合は、ステップ７０７において処理を実行する。

【００８６】

この図７に示すフローは特定のサービス端末、例えば銀行のＡＴＭ等を想定した場合の処理フローである。図７のフローにおけるステップ７０５以降の処理は、サービス端末の態様によって異なるものとなる。サービス端末２０が銀行端末である場合、例えば、ステップ７０５の承認応答は、ステップ７０４での出力ＩＤに基づく認証がなされた後のディスプレイへの承認表示処理に相当し、ステップ７０６の処理要求は、例えば引き出し金額の指定要求であり、ステップ７０７の処理実行は、ユーザによる金額指定の処理等に対応する。

【００８７】

また、サービス端末が改札ゲートであるとすると、ステップ７０４において、ユーザの携帯機器から認証用ＩＤの出力がなされると、サービス端末である改札ゲートに接続された端末は、認証の可否に基づいて改札ゲートの開閉を実行することになる。このように、図７の処理フローはサービス端末の提供する処理に応じて異なるものとなる。

【００８８】

次に、図８に基づいてサービス端末側での処理例について説明する。図８の例は、駅の改札のように機器の動作を処理するだけのサービスの例である。ステッ

プ８０１はデータ送信のため、接点２９の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点２９の電位を判定するステップである。接点電位がデータ送信可能状態になると、ステップ８０２において、サービス端末２０からユーザ３０の人体、接点２９を介して携帯機器１０に対してサービスＩＤを送信する。

【００８９】

サービスＩＤを受信した携帯機器１０は、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証用ＩＤを生成し、生成した認証用ＩＤをサービス端末２０に対して出力する。サービス端末２０は、携帯機器１０からの認証用ＩＤを受信すると（ステップ８０３）、ステップ８０４で、受信認証用ＩＤの認証処理を実行する。この処理は、図１における認証部２４が実行する。認証部２４における認証の結果、認証用ＩＤの正当性が判定（ステップ８０５）され、正当であると判定されると、ステップ８０６においてサービス端末に設定されたサービスが実行される。一方、ステップ８０５における判定処理で、正当でないと判定されると、ステップ８０７に進み、サービスは中止され、処理が終了する。

【００９０】

次に、図９に基づいてサービス端末側での異なる処理例について説明する。図９の例は、情報端末のように画像情報、音楽情報等、各種情報を提供するサービスの場合の処理例である。ステップ９０１はデータ送信のため、接点２９の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点２９の電位を判定するステップである。接点電位がデータ送信可能状態になると、ステップ９０２において、サービス端末２０から接点２９、ユーザ３０の人体を介して携帯機器１０に対してサービスＩＤを送信する。

【００９１】

サービスＩＤを受信した携帯機器１０は、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証

用ＩＤを生成し、生成した認証用ＩＤをサービス端末２０に対して出力する。サービス端末２０は、携帯機器１０からの認証用ＩＤを受信すると（ステップ９０３）、ステップ９０４で、受信認証用ＩＤの認証処理を実行する。この処理は、図１における認証部２４が実行する。認証部２４における認証の結果、認証用ＩＤの正当性が判定（ステップ９０５）され、正当でないと判定されると、ステップ９０９においてサービスが中止され、処理を終了する。ステップ９０５において認証用ＩＤが正当であると判定されると、ステップ９０６においてサービス端末に設定されたサービスに規定された処理要求を出力する。さらに、ステップ９０７において、処理要求に対する応答を待機し、応答があった場合は、ステップ９０８において処理を実行し、要求データの送信を行なう。

【００９２】

上述の図８、図９のサービス端末の処理において、例えば図８のフローは、ビルでのセキュリティチェック・サービスの例に相当する。この場合、ステップ８０６のサービスは、ビルのドアの開閉の制御になり、ステップ８０７のサービス中止はドアの開閉処理の中止を意味する。さらに、ステップ８０７のサービス中止に伴う処理として不当ＩＤを登録するとった処理を行う構成としてもよい。

【００９３】

また、図８の処理フローは、交通システム精算サービスの例に相当し、この場合ステップ８０６のサービスは改札ゲートの開閉をコントロールするだけでなく、料金精算が必要な場合には、電子精算処理も行う構成とすることができる。

【００９４】

また、図８の処理フローは、携帯電話、ディスプレイを有する携帯端末の利用携帯としても適用可能である。例えば、図１０に示す（ａ）携帯電話や、（ｂ）ＰＤＡ等のディスプレイ機器などを利用した処理が可能である。ここで図１０（ａ）の携帯端末は導電性の接点を具備することを特徴とするサービス端末であり、図１０（ｂ）ディスプレイ端末は、導電性のあるジョグダイヤルを具備することを特徴とするサービス端末である。

【００９５】

図１０（ａ）の携帯電話において、図８のサービス端末の処理を実行する場合

、サービス端末としての携帯電話を複数人で使う利用形態において、ユーザの識別データを腕時計等の携帯機器から携帯電話にユーザの人体を介して転送し、認証用ＩＤの正当性が確認された場合のみ携帯電話の使用が可能となる構成が実現される。この場合の図８のステップ８０６のサービスは通話可能モードへの設定処理となる。なお、携帯電話のディスプレイ領域に認証用ＩＤに相当する電話番号リストを表示するようにしてもよい。また、図１０（ｂ）のＰＤＡ等のディスプレイ機器の場合には、オンラインショッピングを行う場合に、認証用ＩＤをベースにして、サービスプロバイダとの認証を行い決裁を行うシステムとしての利用が考えられる。

【００９６】

さらに、図９に示した処理フローを実行するサービス端末の例としてリモート機器制御機器がある。例えば、病院等では電波を発生するために携帯電話の使用が制限されている。このような状態で、ベッドから移動することができないような患者に対して、電話機器を利用することができるようなサービスを提供する端末が実現される。

【００９７】

図１１を用いて図９に示した処理フローを実行するサービス端末の例について説明する。患者４０が表示部を持つ腕時計タイプの携帯機器４１を身につける。患者４０が電話をかけたいときは、壁から吊り下げられたワイヤー状の接点４２に触れることにより、壁４３に埋め込まれたサービス端末４４あるいは、壁４３を通じて遠隔地に存在するサービス端末４４と通信を行う。

【００９８】

患者４０がワイヤー状の接点４２を持つことにより、サービス端末４４からサービスＩＤが送信（ステップ９０２）され、これに応答して、携帯機器４１から認証用ＩＤが携帯機器に送られて、サービス端末４４において認証用ＩＤの正当性チェックが実行（ステップ９０４）される。

【００９９】

認証処理で正当性が確認されると、処理要求、すなわち、電話番号データの出力を患者４０に要求（ステップ９０６）する。電話番号データは、患者による音

声出力、あるいは携帯機器４１に構成した電話番号データ入力キー等によって行なうことが可能な構成とし、これらの電話番号を受信したサービス端末４４は、電話を接続する処理を実行（ステップ９０８）する。この構成において、サービス端末４４には、モデムの機能が内蔵されている。サービス端末４４はさらに構内回線４５を通じてデジタル交換器４６と接続しており、この交換器４６から外部公衆回線網４７を通じて外部に電話をかけることが可能となる。

【０１００】

サービス端末４４が留守番電話の機能を有するようにすれば、患者がワイヤー状の接点４２を持つことにより、その情報を携帯機器４１に受信し、接点４２を離した後で、携帯機器４１の再生機能を使って、情報を再生することも可能である。

【０１０１】

［実施例２］

次に図１２に示すように、認証情報通信システムが、ユーザ３０が装着した携帯機器１００と、サービス提供端末１１０と、サービス登録端末１２０、並びに認証課金等のユーザ管理を行うのためのクリアリングハウス１３０とから構成されたシステム構成例について、第２実施例として説明する。

【０１０２】

図１２に示すシステムは、サービス提供端末１１０からのサービスを受けるユーザに対して、ユーザの認証処理のみならず、ユーザ毎に使用可能なサービスを設定するとともに、サービス利用状況を把握して、ユーザ単位の課金を可能としたシステムである。

【０１０３】

サービス提供端末１１０は、実際のサービスを提供する端末、例えば、音楽、画像情報等のコンテンツ情報の提供端末、あるいは遊園地の改札ゲート、駅の改札ゲート等、様々な場所に設置された様々なサービスを提供する端末である。なお、図１２には、サービス端末１１０が１つのみ記載されているが、サービス端末１１０はネットワーク１４０を介して複数台、必要な位置、例えばサービス端末が改札ゲートの開閉処理を実行する場合はそれぞれのゲート位置に配置されて

いるものであり、図１２では、複雑化を避けるために１つの構成のみを記載していることを理解されたい。

【０１０４】

サービス提供端末１１０のＣＰＵ１１１は、ＲＡＭ１１３格納情報をサービス提供端末１１０の通信部２，１１５から携帯機器１００の通信部に送付し、データを受信した携帯機器１００は、携帯機器１００内のＲＡＭ等の記憶回路に受信データを蓄えることができる。なお、通信部１，１１４は、サービス登録端末１２０、クリアリングハウス１３０との通信用である。さらに、サービス提供端末１１０のＲＯＭ１１２には、それぞれの装置の基本的な制御を行うＯＳやデバイスドライバなどの基本ソフトウェアが記憶されており、ＣＰＵ１１１によって読み出されそれぞれの装置を機能させることができる。

【０１０５】

サービス登録端末１２０は、ユーザ３０が、サービス提供端末１１０からのサービスを受けるために必要な登録を行なうための端末であり、例えばサービス提供端末１１０が駅の改札ゲートであれば、サービス登録端末１２０は定期券、切符等の販売を行なう駅に設置され、サービス提供端末１１０が遊園地の改札ゲートであればサービス登録端末１２０は入場券販売所等に設置される。また、サービス登録端末１２０が音楽、画像情報等のコンテンツ情報の提供端末であれば、サービス登録端末１２０は、例えばコンビニエンスストアや駅などに設置されている情報提供端末、ＡＴＭのような装置として構成することができる。

【０１０６】

サービス登録端末１２０のＣＰＵ１２１は、ＲＡＭ１２３格納情報をサービス登録端末１２０の通信部２，１２５から携帯機器１００の通信部に送付し、データを受信した携帯機器１００は、携帯機器１００内のＲＡＭ等の記憶回路に受信データを蓄えることができる。なお、通信部１，１２４は、サービス提供端末１１０、クリアリングハウス１３０との通信用である。サービス登録端末１２０のＲＯＭ１２２には、それぞれの装置の基本的な制御を行うＯＳやデバイスドライバなどの基本ソフトウェアが記憶されており、ＣＰＵ１２１によって読み出されそれぞれの装置を機能させることができる。

【０１０７】

サービス登録端末１２０は、登録処理のための入出力機器、例えば、情報出力、入力用のディスプレイ、マイク、スピーカ等を備えている。携帯機器１００を装備したユーザ３０は、サービス登録端末１２０との通信においてもサービス登録端末１２０に設定された接点１２８を介した通信を実行する。携帯機器１００を装着したユーザ３０が接点１２８においてサービス登録端末１２０に接触し、サービス登録端末１２０の接点１２８の電位が上昇し、通信可能な状態になると、サービス登録端末１２０は、まずユーザに対して、サービスの選択処理を実行することを要求する。

【０１０８】

サービス登録端末１２０のサービス選択部１２７は、ユーザに対してサービス登録端末１２０に構成されたディスプレイ、またはサービス登録端末１２０に接続されて配置されたディスプレイに図１３に示すようなメッセージ２０１を表示し、選択画面２０２中のサービス項目の中の一つを選択するように促す。

【０１０９】

ユーザ３０が、図１３に示すディスプレイの選択画面２０２からタッチ入力、あるいはキーボード入力、音声入力、その他の入力手段によりサービス項目の一つを選択すると、サービス登録端末１２０は、ユーザ３０に対してユーザ３０の選択したサービスに対応するサービス識別子を通信部２，１２５、接点１２８を介して、ユーザ３０の装着した携帯機器１００に送付する。

【０１１０】

サービス識別子を受信したユーザ３０の携帯機器１００は、実施例１と同様に、可変データ記憶部１７（図１、図４参照）で可変ユーザＩＤを選択する。このとき、ユーザ３０が以前に一度も当該サービスを利用していなければ、この可変ユーザＩＤは初期化された値（例えば０）になっている。

【０１１１】

さらに、ユーザ３０の携帯機器１００の合成部１４（図１、図４参照）で固定データ記憶部のデータ、すなわち予めユーザに対する固定値として設定されている固定ユーザＩＤと先述した可変データ記憶部１７に記憶されたサービスに対応

する可変ユーザＩＤが合成されて生成されたサービス固有のユーザ識別子が、サービス登録端末１２０に送信され、通信部２，１２５において受信される。

【０１１２】

次にサービス登録端末１２０は、通信部１，１２４を使ってクリアリングハウス１３０と通信を行うことにより、ユーザ３０の認証処理を行う。

【０１１３】

クリアリングハウス１３０は、サービス提供端末１１０と、サービス登録端末１２０との通信を実行する通信部１，１３４、基本的な制御を行うＯＳやデバイスドライバなどの基本ソフトウェアが記憶されたＲＯＭ１３２、ＣＰＵ１３１によって実行されるプログラムのワークエリアと、入力されたデータなどを一時的に記憶するＲＡＭ１３３を有し、ユーザ３０の認証処理を実行する。ユーザ３０の認証処理は、インターネット、あるいはその他の通信回線１４０を介してクリアリングハウス１３０の通信部１，１３４がユーザ３０の認証用データを受信し、受信したデータを認証部１３５に送り、ここで前述の図４によって説明したと同様の処理を実行して認証処理を行う。

【０１１４】

認証処理は、この実施例では、クリアリングハウス１３０の課金認証データ記憶部１３６に記憶された登録テーブルを用いて行なう。クリアリングハウス１３０の課金認証データ記憶部１３６は、例えば図１４に示されるようなデータ構造の登録テーブルを有しており、登録テーブルにユーザ毎の最大使用度数、現在使用度数をセットする構成となっている。図１４に示す登録テーブル１４は一例であり、サービス態様に応じた項目、例えば個々のユーザに設定されたサービス使用期間、サービス使用時間、サービス使用地域、その他のサービスの詳細についての項目を、提供するサービスに応じて設定する。

【０１１５】

ここで、図１４に示す登録テーブルを使用した場合には、ユーザごとの課金認証データ記憶部１３６の登録テーブルの状況として、以下の３つの態様が考えられる。

（１）ユーザ３０は既になんらかのサービスを過去に使った履歴があり、固定ユ

ーザＩＤが一致するレコードが課金認証データ記憶部１３６に存在しているが、今回の要求サービスに対応するレコードは存在しない。

（２）ユーザは、今回要求したサービスと同じサービスを過去に利用したことがあるので、対応する固定ＩＤレコードが存在する。

（３）ユーザは一度もサービスを利用したことがないので、ユーザのＩＤは登録されていない。

【０１１６】

上述の各態様において、（１）または（３）の場合は、ユーザ３０から要求のあったサービスに対してユーザ登録が新たに必要となるので、登録処理要求をサービス登録端末１２０に通知し、サービス登録端末１２０は、ユーザ３０から要求のあったサービスに対するユーザ登録処理を実行する。具体的には、ユーザ識別子生成部１２６において当該ユーザに対応するユーザ識別子（可変ユーザ識別子）を生成し、当該サービスのサービス識別子とともに、通信部２，１２５から接点１２８、ユーザ３０を介してユーザの携帯端末１００に送信する。ユーザ３０の携帯端末１００では、受信したサービス識別子と可変ユーザ識別子との対を可変データ記憶部１７に対応させて記憶する（図４参照）。

【０１１７】

サービス識別子と、このサービス識別子に対応する可変ユーザ識別子とを、携帯機器１００の可変データ記憶部１７に登録したユーザは、その後、携帯端末１００の合成部１４で、固定データ記憶部の固定ユーザ識別子と今受信した可変ユーザ識別子とを合成し、サービス固有のユーザ識別子を生成して、これをサービス登録端末１２０に送付することによって、サービス登録端末１２０にユーザ登録処理の実行を依頼する。

【０１１８】

ユーザ登録依頼を受け取ったサービス登録端末１２０は、次にクリアリングハウス１３０に対して、受信したサービス固有のユーザ識別子を転送することにより、ユーザ登録を依頼する。このサービス固有のユーザ識別子データを受信したクリアリングハウス１３０は、自身の課金認証データ記憶部１３６に対して、当サービス固有のユーザ識別子に相当するレコードを作成し、最大使用度数を所定

の数値にセットすると共に、現在使用度数を０として初期化する。

【０１１９】

上述の手続きを実行し、ユーザ登録が完了したユーザ３０は、サービス固有のユーザ識別子を携帯機器１００の可変データ記憶部に保持することになり、要求したサービスをサービス提供端末１１０を介して受けることができる。

【０１２０】

サービス提供を受けようとするユーザ３０は、サービス提供端末１１０の接点１１６に触れ、サービス提供端末１１０から、接点１１６、ユーザ３０の人体を介して携帯機器１００に対するサービス識別子の転送を受ける。携帯機器１００は、これに応答して、登録した可変ユーザＩＤと固定ユーザＩＤを合成し、サービス固有のユーザ識別子を生成して、これをサービス提供端末１１０に転送する。

【０１２１】

さらに、このサービス固有のユーザ識別子が、クリアリングハウス１３０にネットワーク等を介して転送されて、認証処理、および課金認証データ記憶部１３６の登録テーブルの使用度数の更新が行なわれる。認証処理は、前述の実施例と同様の処理となる。ユーザ３０は、このような手続きを経て、使用度数に至るまでサービス提供端末１１０からのサービスを受けることができる。

【０１２２】

次に（２）の場合、すなわち、今回要求したサービスと同じサービスを過去に利用したことがあり、対応する固定ＩＤレコードが登録テーブルに存在する場合の処理について説明する。（２）の場合は、さらに、次の２つのケースが考えられる。（２－１）まだ現在使用度数が最大使用度数を超えていない。（２－２）すでに現在使用度数が最大使用度数を超えている。

【０１２３】

（２－１）の場合には、クリアリングハウス１３０は、サービス登録端末１２０に対して、「登録の必要がない」という意味のメッセージを送付する。サービス登録端末１２０は、このメッセージを受信することにより、ユーザ３０に対して、その旨通知して、処理を終了する。（２－２）の場合には、クリアリングハ

ウス１３０は、サービス登録端末１２０に対して、「更新の必要あり」という意味のメッセージを送付する。サービス登録端末１２０は、このメッセージを受信することにより、ユーザ３０に対して、その旨通知して、ユーザ３０に対して、更新するかどうかの問い合わせを行う。ユーザ３０が更新に同意する場合には、クリアリングハウス３０に対して、更新処理を依頼する。

【０１２４】

クリアリングハウス３０における更新処理は、具体的には、例えば、課金認証データ記憶部１３６の登録テーブルの対応するレコードの現在使用度数を０にセットする処理である。ユーザ３０が更新に対して同意しない場合には、さらにユーザ３０に対して、課金認証データ記憶部１３６の登録テーブルのレコードを削除するかどうかの問い合わせを行う。ユーザ３０がレコード削除に同意した場合には、クリアリングハウス３０に対して、当該レコードの削除を依頼し、クリアリングハウス３０は当該レコードを課金認証データ記憶部１３６から削除する。ユーザ３０がレコード削除に同意しない場合には、サービス登録端末１２０はそのまま処理を終える。

【０１２５】

携帯端末１００を所持するユーザ３０が、サービス提供端末１１０に接点１１６で接触してサービスの提供を受ける場合の処理について説明する。サービス提供端末１１０にはサービスを提供するためのデータ入出力機器としての表示ディスプレイ１１８、マイク１１９が付属しており、サービス開始の際には、表示ディスプレイ１１８に、例えば図１５に示すような案内表示がなされる。表示ディスプレイにはサービス選択画面３０１が示される。

【０１２６】

ユーザ３０がサービス提供端末１１０の接点１１６に接触すると、サービス提供端末１１０は、サービス識別子記憶部１１７のデータを読出し、ユーザ３０の携帯端末１００に対してサービス識別子を通信部２，１１５、接点１１６、ユーザ３０の人体を介して送信する。

【０１２７】

図４を用いてこのサービス識別子受信後の処理を説明する。サービス識別子が

「０１０」であったとする。この場合、携帯機器１００の可変データ記憶部１７においてサービス識別子「０１０」に相当するレコードには可変ユーザ識別子として「０００１００１１」が記憶されているので、これを、固定データ記憶部１６に記憶されている固定ユーザ識別子「１０１０００００」と合成部１４において合成処理を実行し、例えば、「１０１０００００００１００１１」というデータを生成する。

【０１２８】

このデータは、サービス固有のユーザ識別子であり、これをサービス提供端末１１０に送付する。当該データを受信したサービス提供端末１１０は、その後このデータをクリアリングハウス１３０に送付することによって、ユーザ認証・課金処理を依頼する。クリアリングハウス１３０では、サービス提供端末１１０から送信されたサービス固有のユーザ識別子データを受信すると、認証部１３５において、サービス固有のユーザ識別子に基づいて、固定ユーザ識別子「１０１０００００」と可変ユーザ識別子「０００１００１１」を分離生成する処理を実行したのち、課金認証データ記憶部１３６にアクセスしてユーザが登録されているかどうかの認証を行う。

【０１２９】

その後、課金認証データ記憶部１３６にて図１４にあるような登録テーブルを用いて認証が正しくなされた場合には、サービス提供端末１１０に対して「認証ＯＫ」のメッセージを送信すると同時に、課金認証データ記憶部の当該レコードの現在使用度数を１減少させる。クリアリングハウス１３０から「認証ＯＫ」のメッセージを受信したサービス提供端末１１０では、サービスが提供される。

【０１３０】

クリアリングハウス１３０において認証が失敗した場合には、サービス提供端末１１０に付属するディスプレイ装置１１８等に「認証が失敗した」旨を通信するメッセージを表示することによって、処理を終了する。

【０１３１】

以上の例において、通信中のデータの安全性を考慮して、各構成要素の通信部１，１１４，通信部２，１１５，通信部１，１２４，通信部２，１２５，及び通

信部１，１３４から送出されるデータは暗号化装置によって暗号化されて送出されるようにし、各通信部において受信された後に復号するようにしてもよい。

【０１３２】

上述の例は、サービス提供端末１１０がディスプレイを使用した情報提供を主に実行する構成の例であるが、ユーザの受けようとするサービスが駅、遊園地等の改札ゲートの開閉動作であってもよく、この場合、サービス提供端末１１０は、各駅、あるいは遊園地の複数の場所に設置された改札ゲートとして構成される。この場合、図１２のサービス提供端末１１０は、各ゲートに対応して配置される。ユーザ３０はサービス提供端末１１０の接点１１６に触れ、合成処理により生成されたサービス固有のユーザ識別子、この場合は、定期券の所定区間、所定期間に対応する改札開閉処理サービス固有のユーザ識別子をサービス提供端末１１０、クリアリングハウスに転送し、認証処理、課金または清算処理を行ない、有効な認証処理がなされた場合のみ、改札ゲートをオープンさせる。

【０１３３】

認証処理は先に説明したように、ユーザの装着した携帯機器１００とサービス提供端末とのユーザ３０を介した通信を実行して行われる。従って、接点１１６は、各ゲートに設置された接点である。携帯機器１００を装着したユーザ３０が接点１１６を触れることで、認証処理が実行され、認証がなされた場合は、ゲートがオープンする。

【０１３４】

この場合、サービス登録端末１２０は、ユーザ３０がサービスを受けるために必要な登録を行なうための端末であり、定期券、切符等の販売を行なう駅、あるいは、入場券販売所等に設置される。

【０１３５】

サービス登録端末１２０での登録処理は、ユーザ３０がサービス登録端末１２０の接点１２８に触れることによって開始される。サービス登録端末１２０において、ユーザ３０は、特定のサービス、例えば、定期券の販売であれば、駅区間、有効期間の設定を行ない、これらの設定区間、期間のデータを前述のクリアリングハウス１３０の課金認証データ記憶部１３６の登録テーブル中に登録し、登

録テーブルを参照してユーザの認証処理を実行する。このように、サービス提供端末の提供するサービスは各種可能であり、サービス単位、かつユーザ単位の認証処理、管理が可能となる。

【０１３６】

なお、以上の説明では、基本的に認証を行う携帯機器についての例を述べたが、認証が不要な応用例、例えば、本携帯機器の認証機能をオフ、あるいはすべてのユーザを無条件に認証するとした設定とすることで、情報交換機器としても利用、すなわち外部情報入力システムとしての応用が可能である。例えば、電車内での所定の位置、例えば、公告の一部、または吊革等に接点を構成することで、携帯機器を有するユーザがこれらの接点に接触することで、電車内の広告情報が携帯機器に入力されるようにすることができる。携帯機器中のメモリに情報を取り込んだり、あるいは携帯機器に付属するディスプレイ、スピーカを通じて情報を出力する構成としてもよい。

【０１３７】

さらに、図１６のように、腕時計型あるいはブレスレット型の携帯装置２０１、２０２を装着した２人のユーザが、携帯装置２０１、２０２をそれぞれ装着して握手を行なうことにより、携帯装置２０１と携帯装置２０２の間で、握手した人体を介するデータ転送を行なうことが可能である。また、携帯装置２０１と携帯装置２０２内に認証処理構成を内蔵させれば、認証された携帯機器を有する者同士では、情報を転送することが可能であるが、認証されない相手に対しては、情報の転送が実行されない構成とすることができる。

【０１３８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１３９】

【発明の効果】

以上の説明から明らかなように、本発明の認証情報通信システムおよび認証情報通信方法によれば、ユーザが装着した携帯機器と、サービスを提供するサービス提供端末間での認証処理を人体を介する通信によって実行し、それぞれの接点に人体が触れることでデータ通信を可能としたので、ユーザが接触したという物理的実感を確認して認証処理が行なわれ、非接触型の認証システムにおける処理の開始確認の曖昧さが解消され、ユーザの不安感が取り除かれるとともに、またカード等の旧来の接触型の認証システムのようなカードの取り出し、センサでの読み取り処理等のわずわらしさもなく、ユーザの負担が軽減される優れた認証処理システムが実現される。

【０１４０】

さらに、本発明の認証情報通信システムおよび認証情報通信方法によれば、ユーザが装着した携帯機器にユーザ固有のユーザ固有識別子と、サービス端末の提供するサービスに応じて各ユーザごとに生成されるユーザ可変識別子とを格納し、サービス端末から送信されるサービス識別子に応じて、携帯端末において、ユーザ固有識別子とユーザ可変識別子とから認証用のサービス固有ユーザ識別データを生成してサービス端末に送付する構成としたので、サービス識別子で規定した内容に応じたユーザ単位の課金処理等、様々なユーザ管理、サービス管理が実行できる認証処理システムが実現される。

【０１４１】

さらに、本発明の認証情報通信システムおよび認証情報通信方法によれば、サービス端末がサービスに応じた可変ユーザＩＤをユーザに対して設定する構成としたので、可変ユーザＩＤのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になり、携帯機器から受信した可変ユーザＩＤに基づいてサービスの実行、態様を変更することが可能となる。

【図面の簡単な説明】

【図１】

本発明の認証情報通信システムの基本構成を示すブロック図である。

【図２】

１ＭＨｚ～３０ＭＨｚの範囲でスペクトラムアナライザを用いて測定した人体

の伝送特性（両手間）を示す特性図である。

【図３】

電解強度とアンテナからの距離との関係を説明する特性図である。

【図４】

本発明の認証情報通信システムの認証処理におけるユーザ側の携帯機器における処理を説明する図である。

【図５】

本発明の認証情報通信システムの認証処理におけるサービス端末における処理を説明する図である。

【図６】

本発明の認証情報通信システムにおける携帯機器の機器構成例を示す図である。

【図７】

本発明の認証情報通信システムにおける携帯機器における処理フローを説明する図である。

【図８】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その１）を説明する図である。

【図９】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その２）を説明する図である。

【図１０】

本発明の認証情報通信システムの使用例（その１）を説明する図である。

【図１１】

本発明の認証情報通信システムの使用例（その２）を説明する図である。

【図１２】

本発明の認証情報通信システムにおける第２実施例の構成を示すブロック図である。

【図１３】

本発明の認証情報通信システムにおける第２実施例のサービス登録端末での処理例を示す図である。

【図１４】

本発明の認証情報通信システムにおける第２実施例の課金認証データ記憶部の登録テーブルの例を示す図である。

【図１５】

本発明の認証情報通信システムにおける第２実施例のサービス提供端末での処理例を示す図である。

【図１６】

本発明の認証情報通信システムにおけるその他の実施例の使用例を示す図である。

【符号の説明】

１０　携帯機器
１１　ＣＰＵ
１２　ＲＡＭ
１３　ＲＯＭ
１４　合成部
１５　通信部
１６　固定データ記憶部
１７　可変データ記憶部
１８　接点
２０　サービス端末
２１　ＣＰＵ
２２　ＲＡＭ
２３　ＲＯＭ
２４　認証部
２５　通信部
２６　認証用ユーザ識別子生成部
２７　認証データ記憶部

２８　サービス識別子保持部

４１　携帯機器

４２　接点

４４　サービス端末

４６　交換機

１１０　サービス提供端末

１１６　接点

１１７　サービス識別子記憶部

１２０　サービス登録端末

１２６　ユーザ識別子生成部

１２７　サービス選択部

１２８　接点

１３０　クリアリングハウス

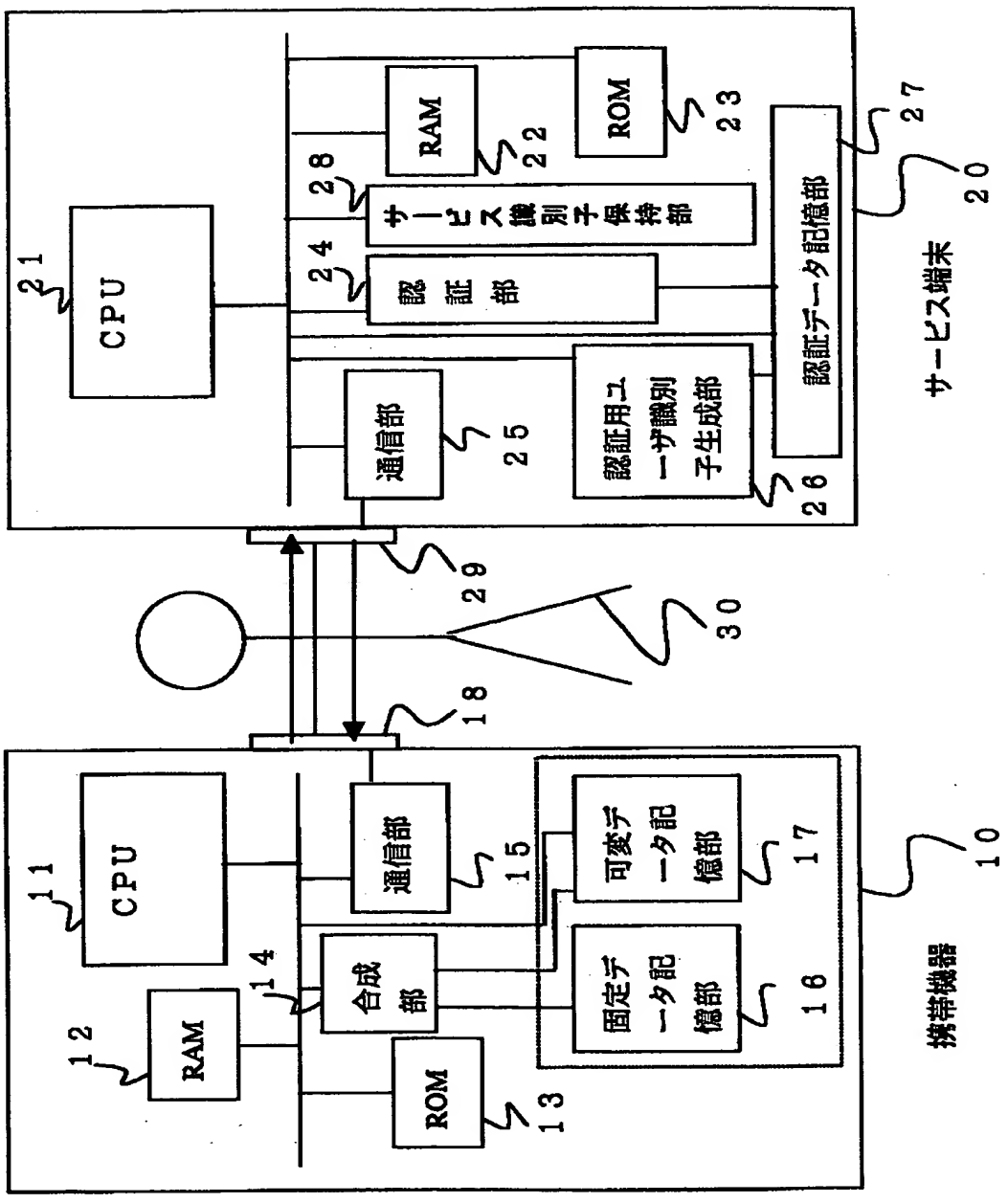
１３５　認証部

１３６　課金認証データ記憶部

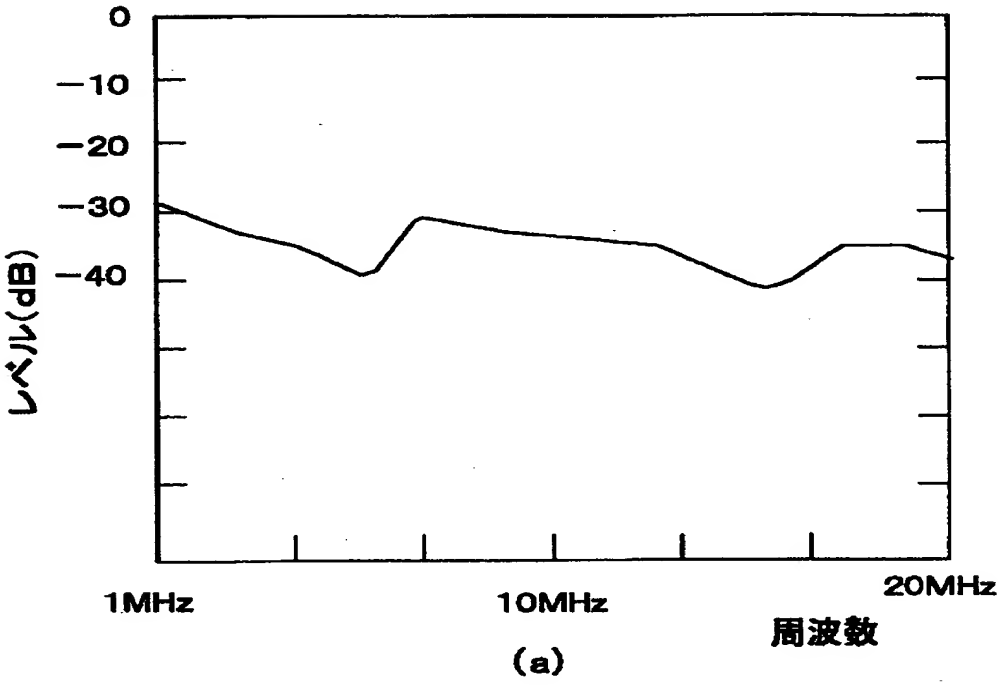
２０１，２０２　携帯装置

【書類名】　　図面

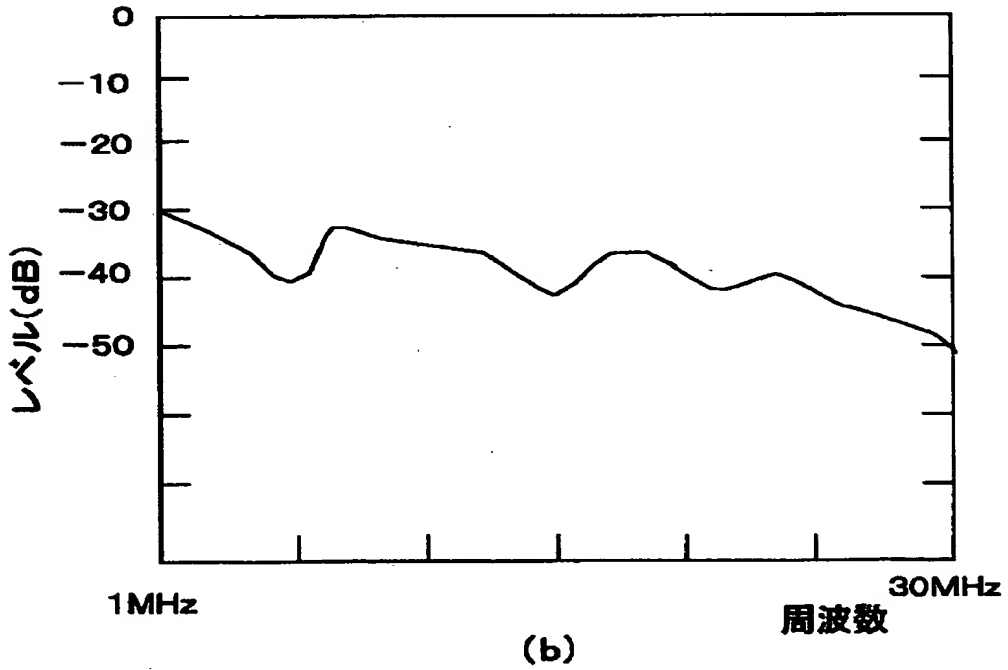
【図１】


CPU
21
RAM
22
ROM
23
28
サービス識別子保持部
24
認証部
通信部
25
認証用ユーザ識別子生成部
26
認証データ記憶部
27
サービス端末
20
29
30
18
CPU
11
RAM
12
14
合成部
ROM
13
通信部
15
可変データ記憶部
17
固定データ記憶部
16
携帯機器
10

【図２】

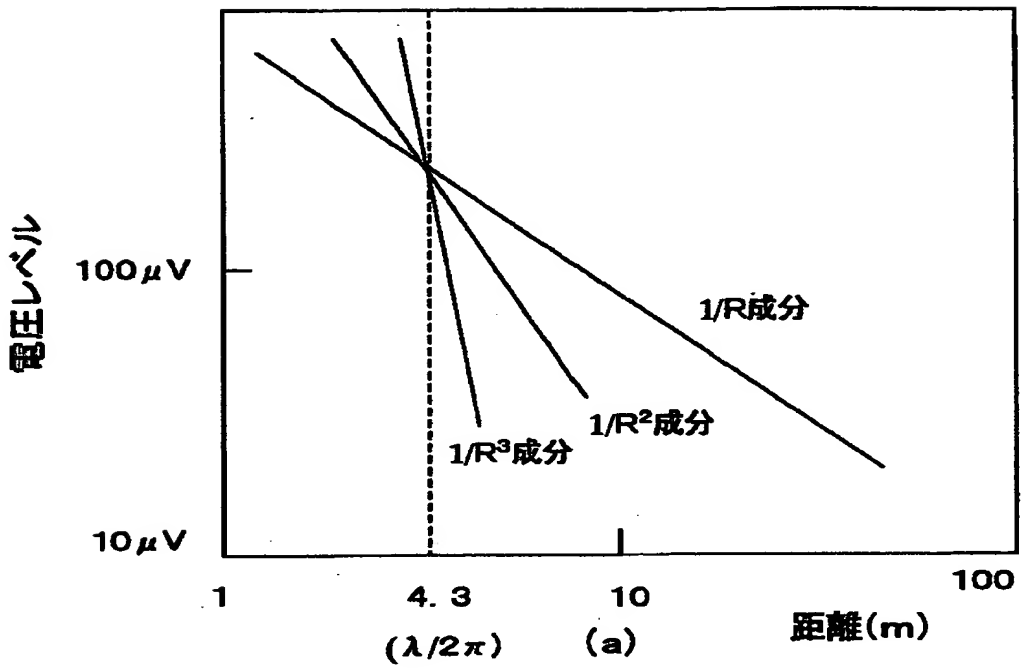

0
−10
−20
−30
−40
レベル(dB)
1MHz
10MHz
20MHz
周波数

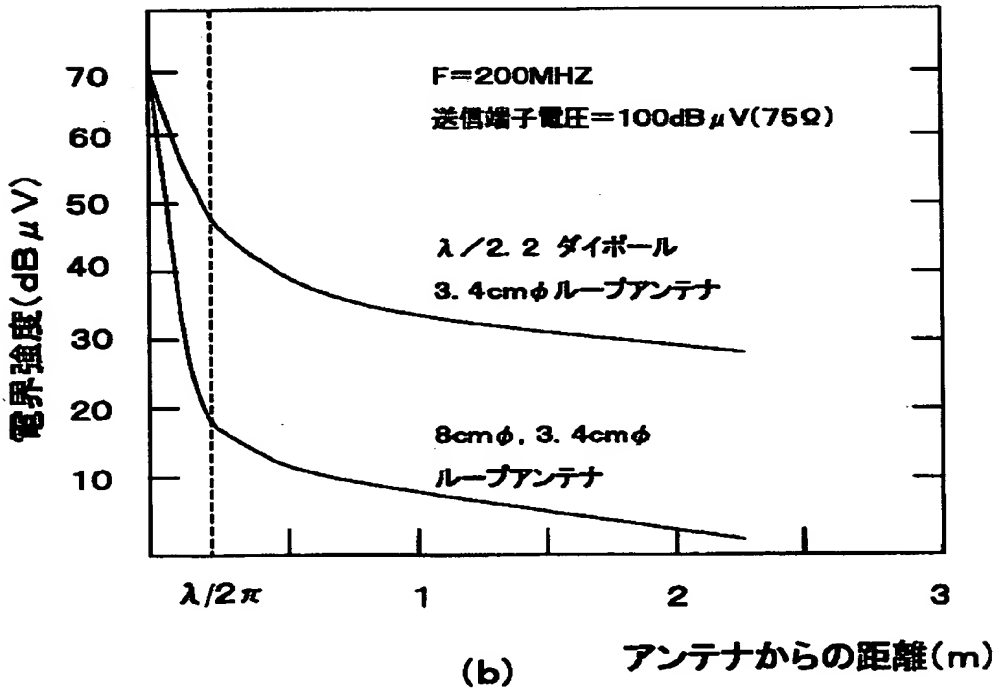
(a)


0
−10
−20
−30
−40
−50
レベル(dB)
1MHz
30MHz
周波数

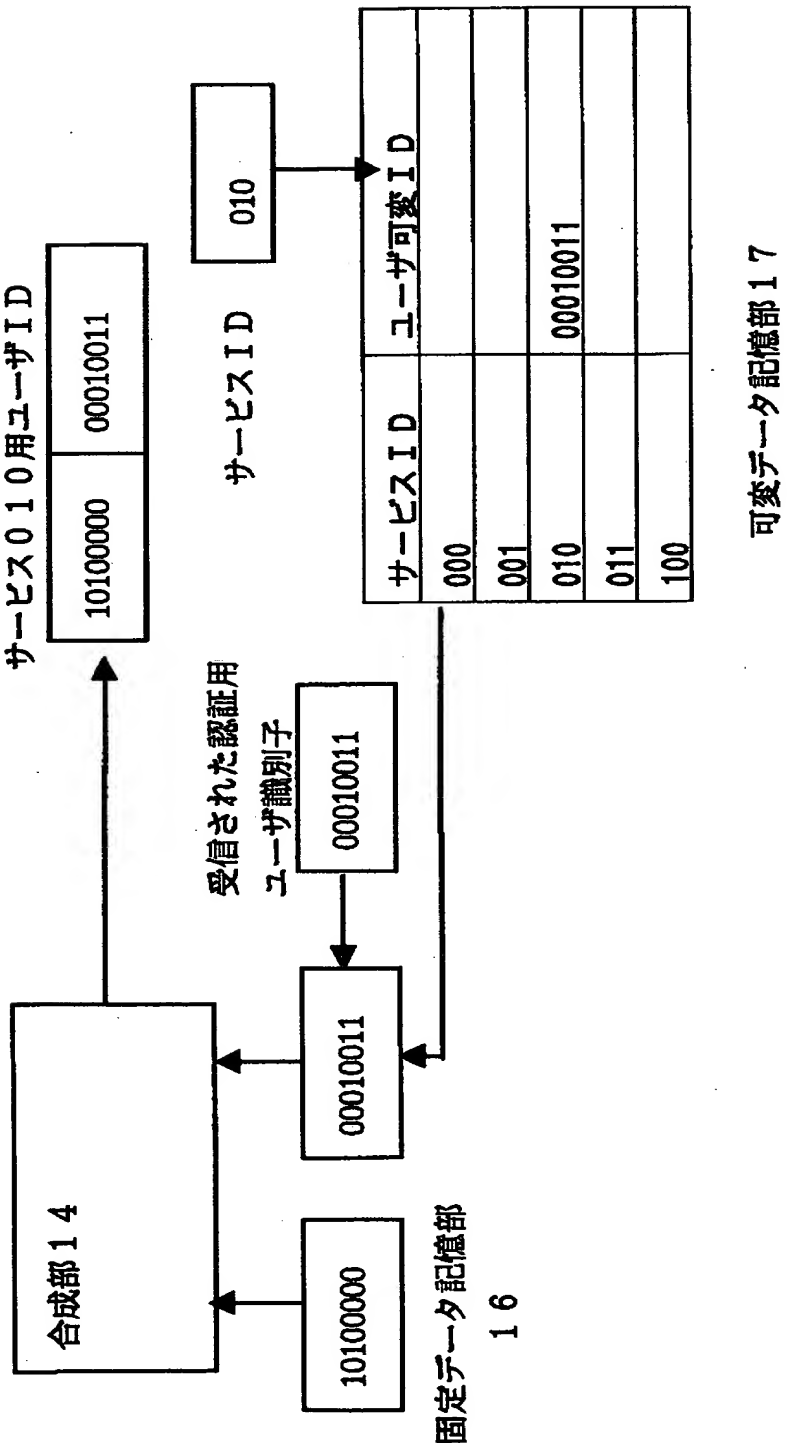
(b)

【図３】

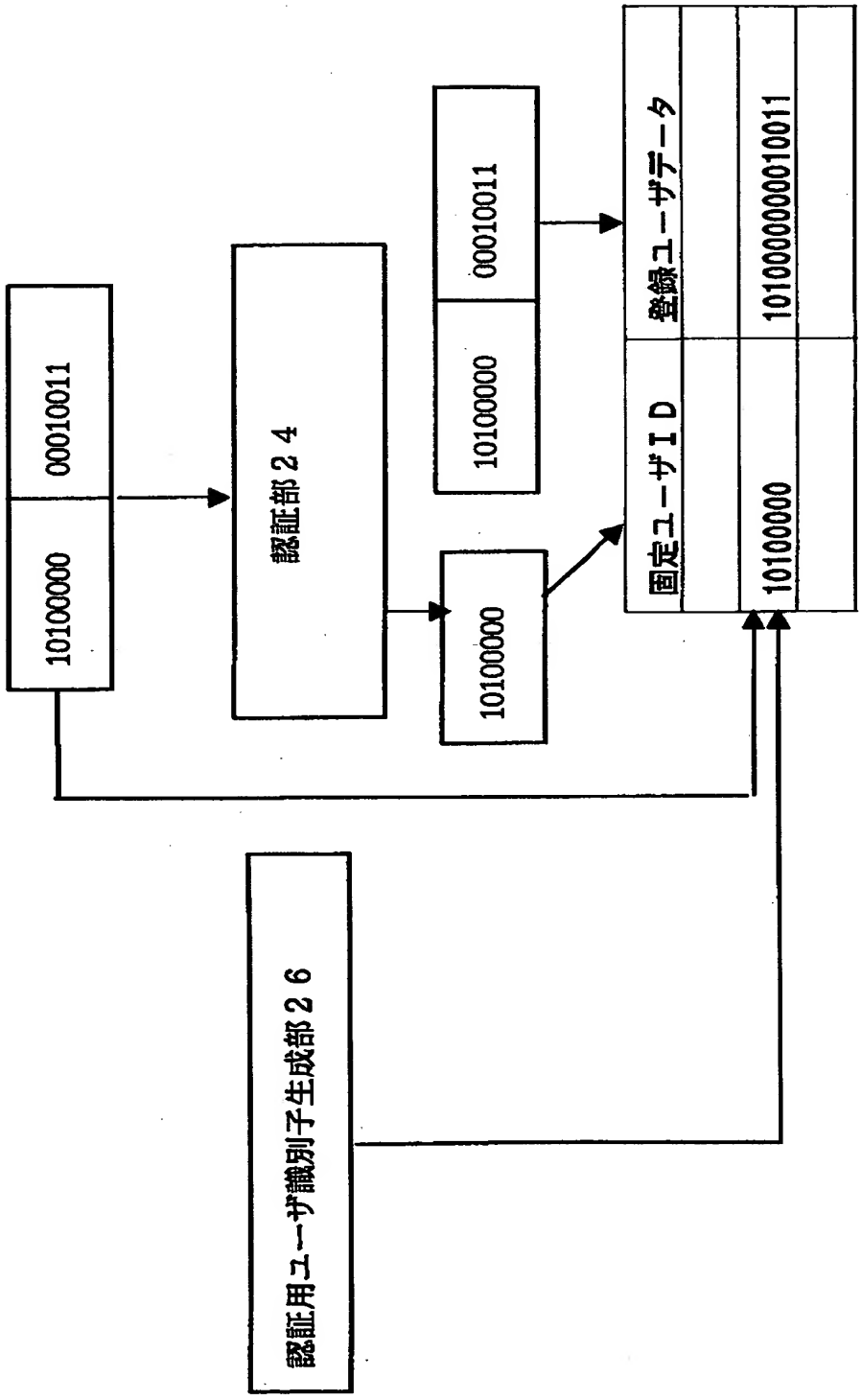

電圧レベル
100μV
10μV
1/R成分
1/R²成分
1/R³成分
1
4.3
(λ/2π)
10
100
(a)
距離(m)


電界強度(dBμV)
70
60
50
40
30
20
10
F=200MHZ
送信端子電圧=100dBμV(75Ω)
λ/2.2 ダイポール
3.4cmφループアンテナ
8cmφ, 3.4cmφ
ループアンテナ
λ/2π
1
2
3
(b)
アンテナからの距離(m)

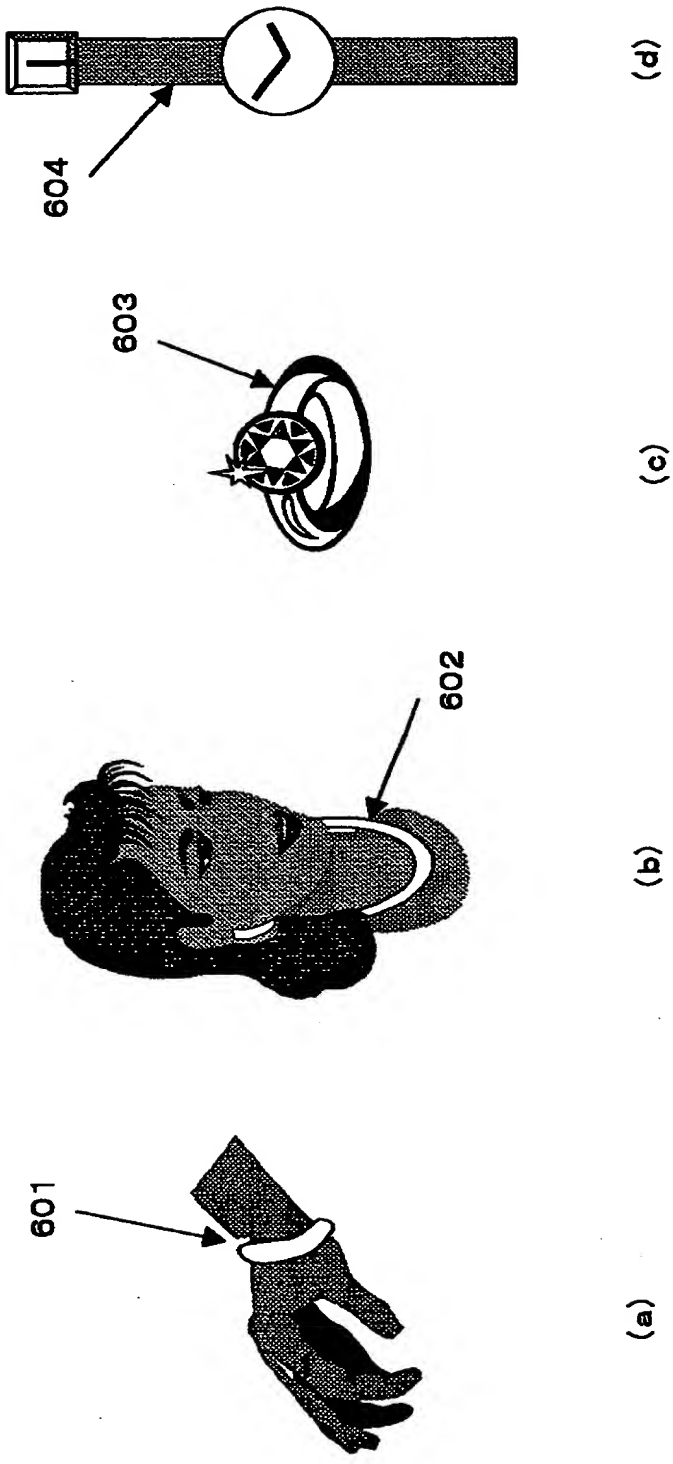
【図４】


サービス０１０用ユーザＩＤ
10100000
00010011
サービスＩＤ
010
サービスＩＤ
ユーザ可変ＩＤ
000
001
010
011
100
00010011
可変データ記憶部１７
受信された認証用
ユーザ識別子
00010011
合成部１４
00010011
10100000
固定データ記憶部
１６

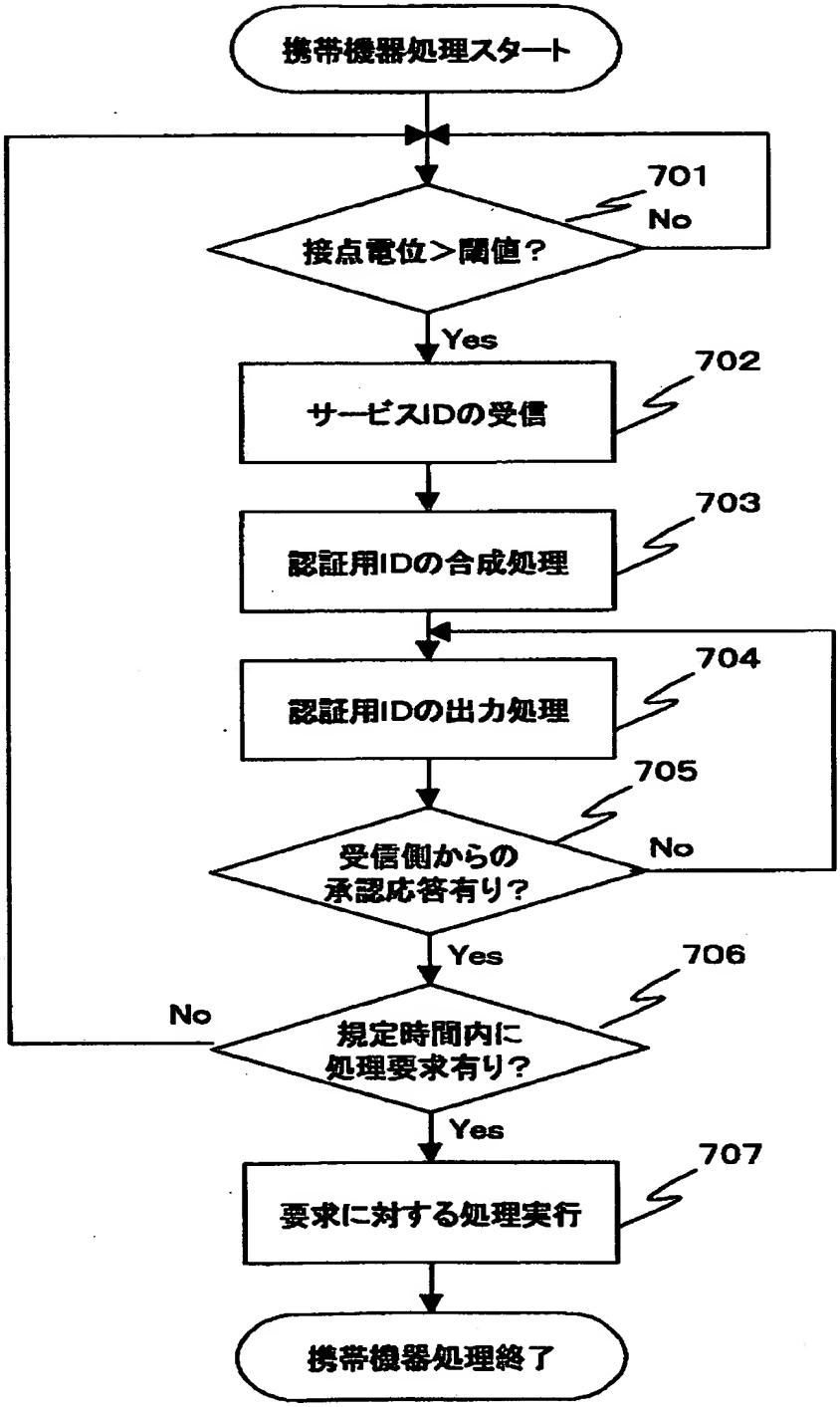
【図５】


00010011
10100000
認証部２４
00010011
10100000
10100000
固定ユーザＩＤ
登録ユーザデータ
10100000
10100000000010011
認証用ユーザ識別子生成部２６

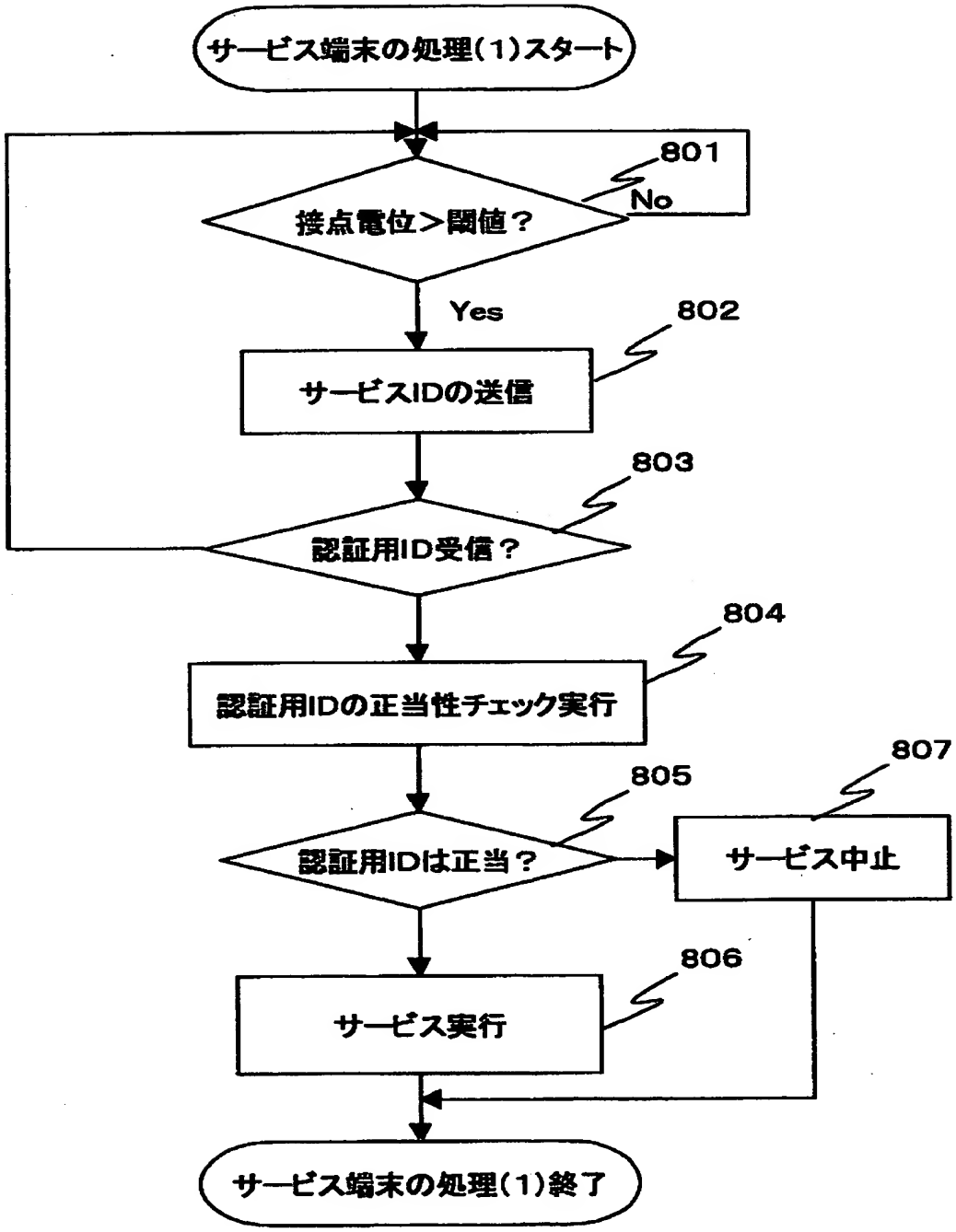
【図６】



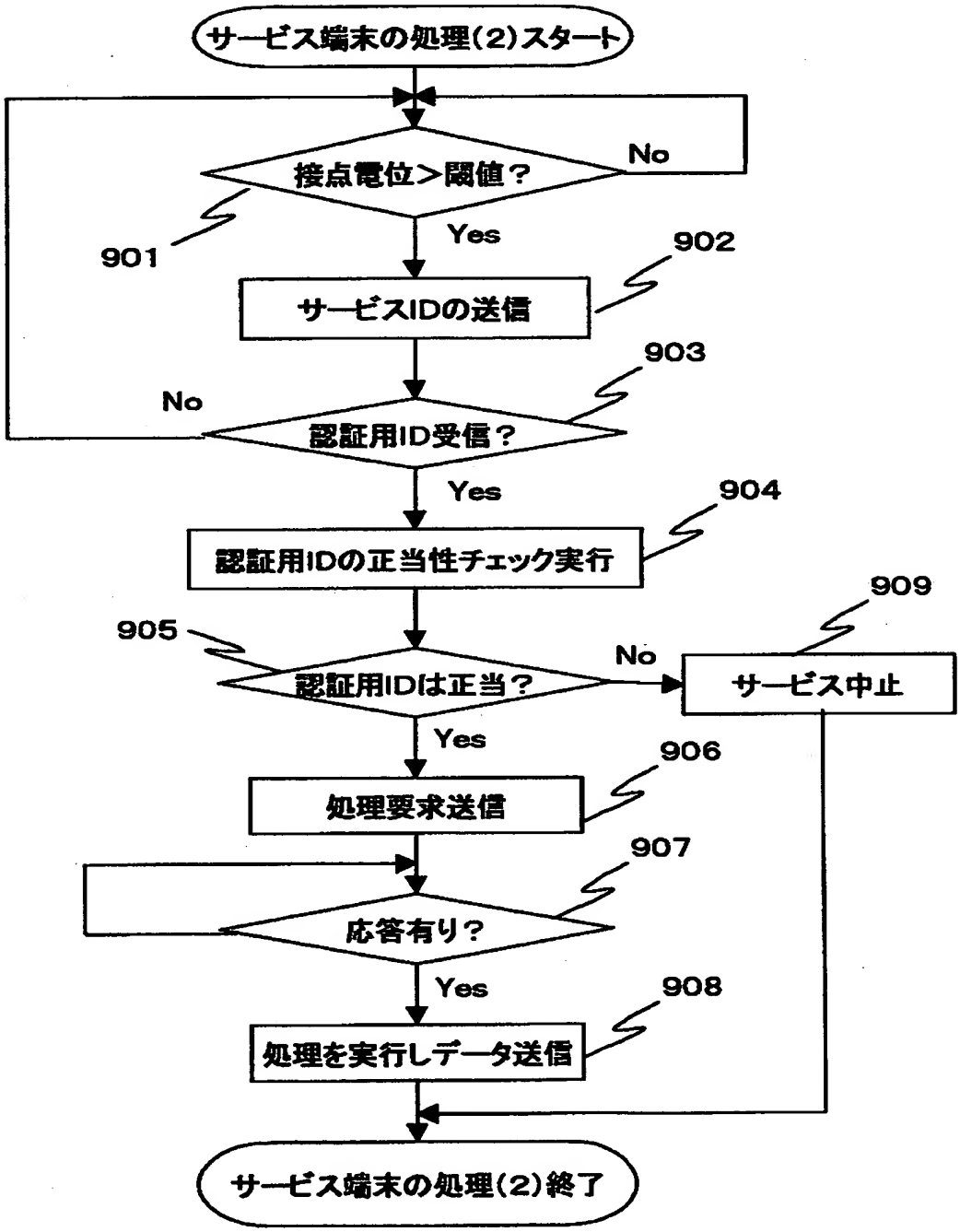
【図７】


携帯機器処理スタート
701
No
接点電位＞閾値？
Yes
702
サービスIDの受信
703
認証用IDの合成処理
704
認証用IDの出力処理
705
No
受信側からの
承認応答有り？
Yes
706
No
規定時間内に
処理要求有り？
Yes
707
要求に対する処理実行
携帯機器処理終了

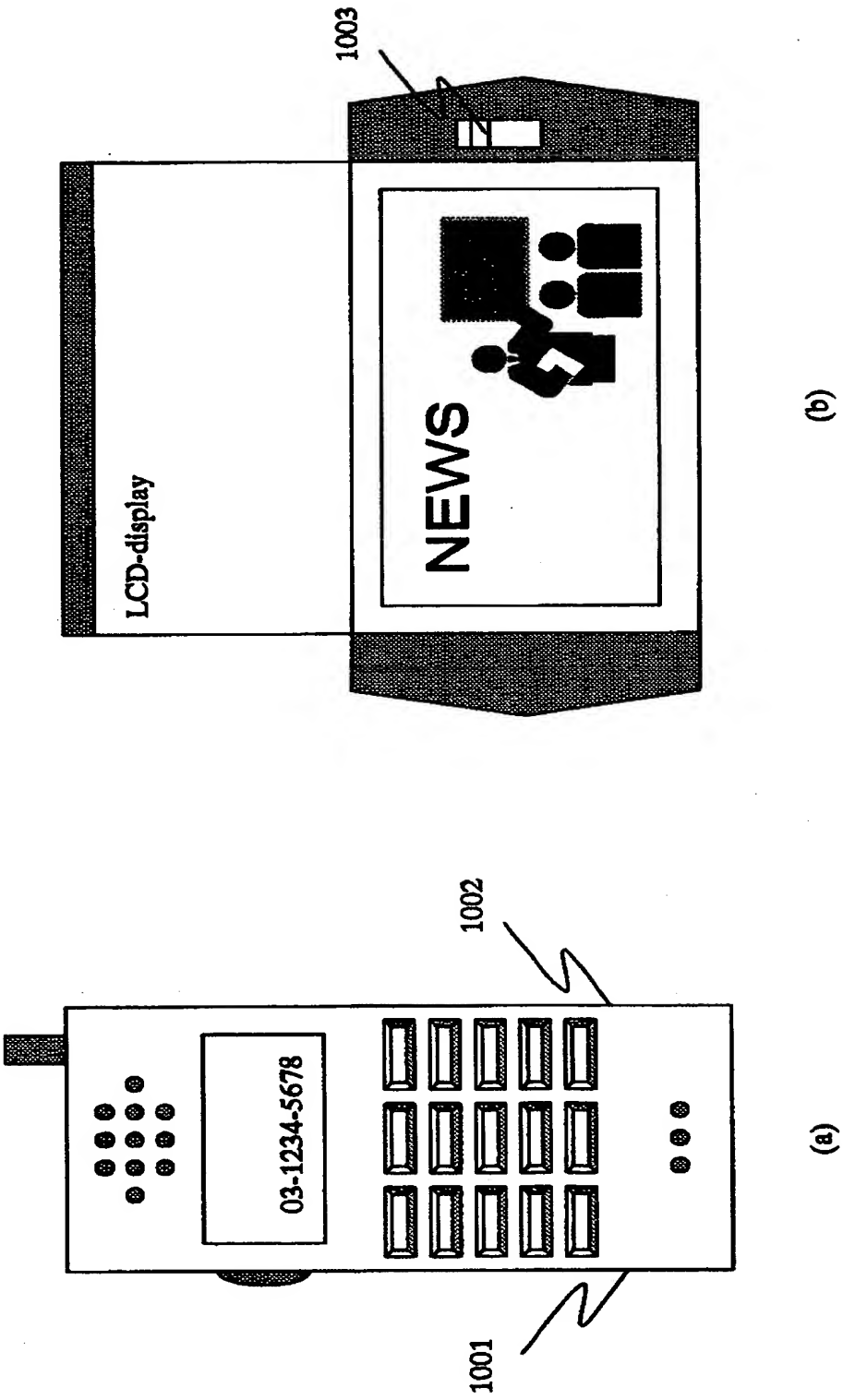
【図８】


サービス端末の処理(1)スタート
801
No
接点電位>閾値？
Yes
802
サービスIDの送信
803
認証用ID受信？
804
認証用IDの正当性チェック実行
807
805
認証用IDは正当？
サービス中止
806
サービス実行
サービス端末の処理(1)終了

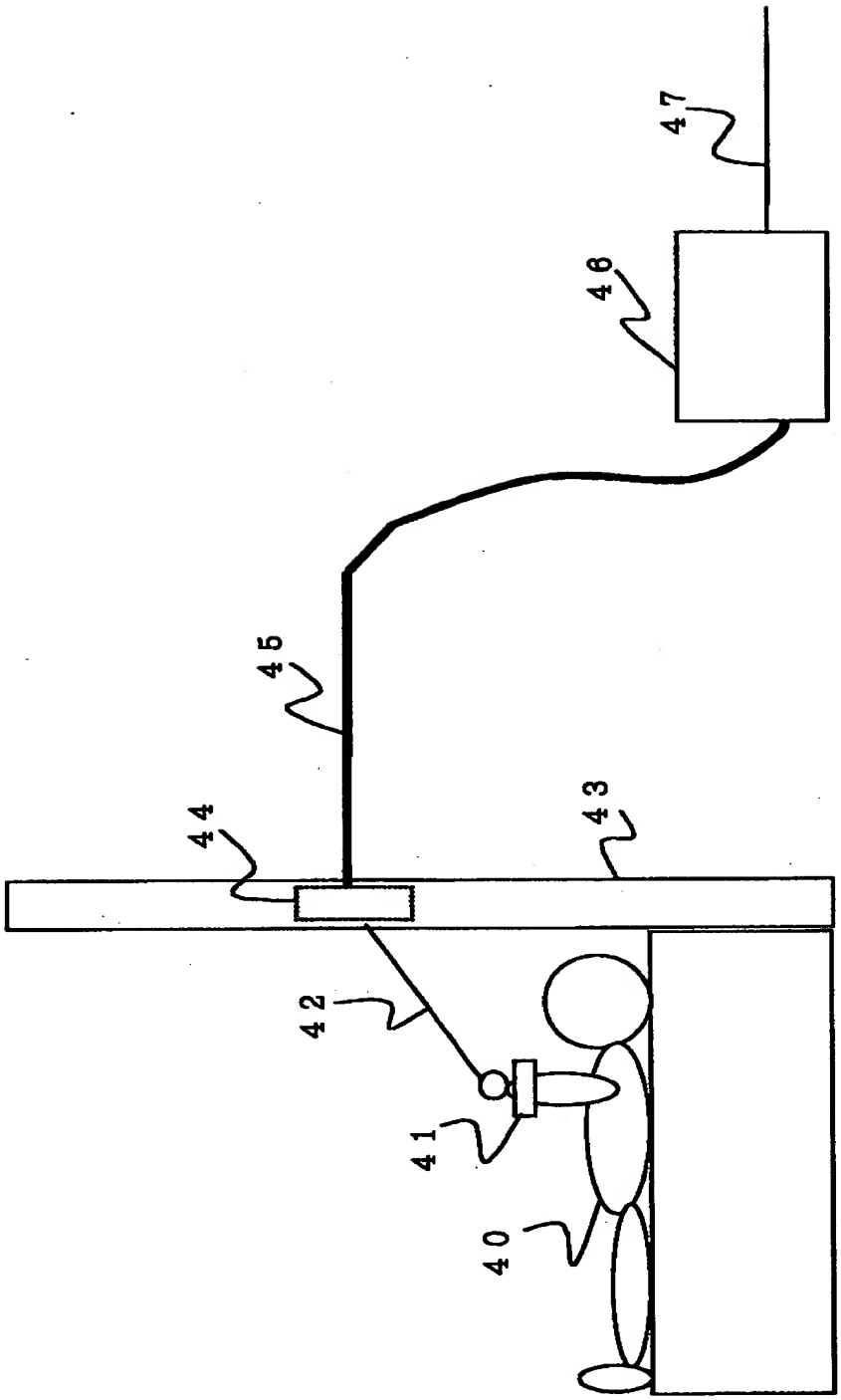
【図９】


サービス端末の処理(2)スタート
接点電位>閾値？
No
Yes
901
902
サービスIDの送信
903
No
認証用ID受信？
Yes
904
認証用IDの正当性チェック実行
905
909
認証用IDは正当？
No
サービス中止
Yes
906
処理要求送信
907
応答有り？
Yes
908
処理を実行しデータ送信
サービス端末の処理(2)終了

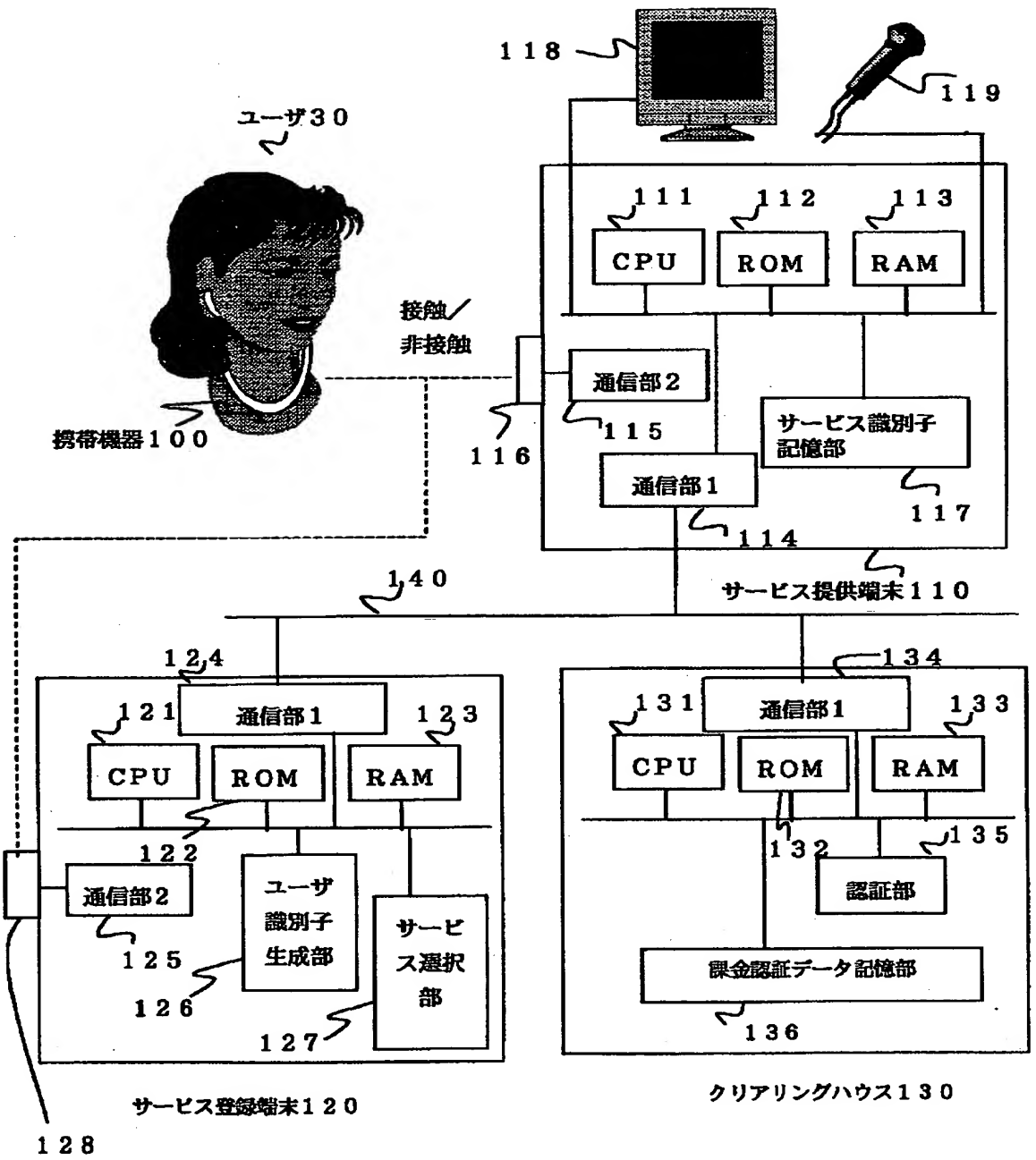
【図１０】



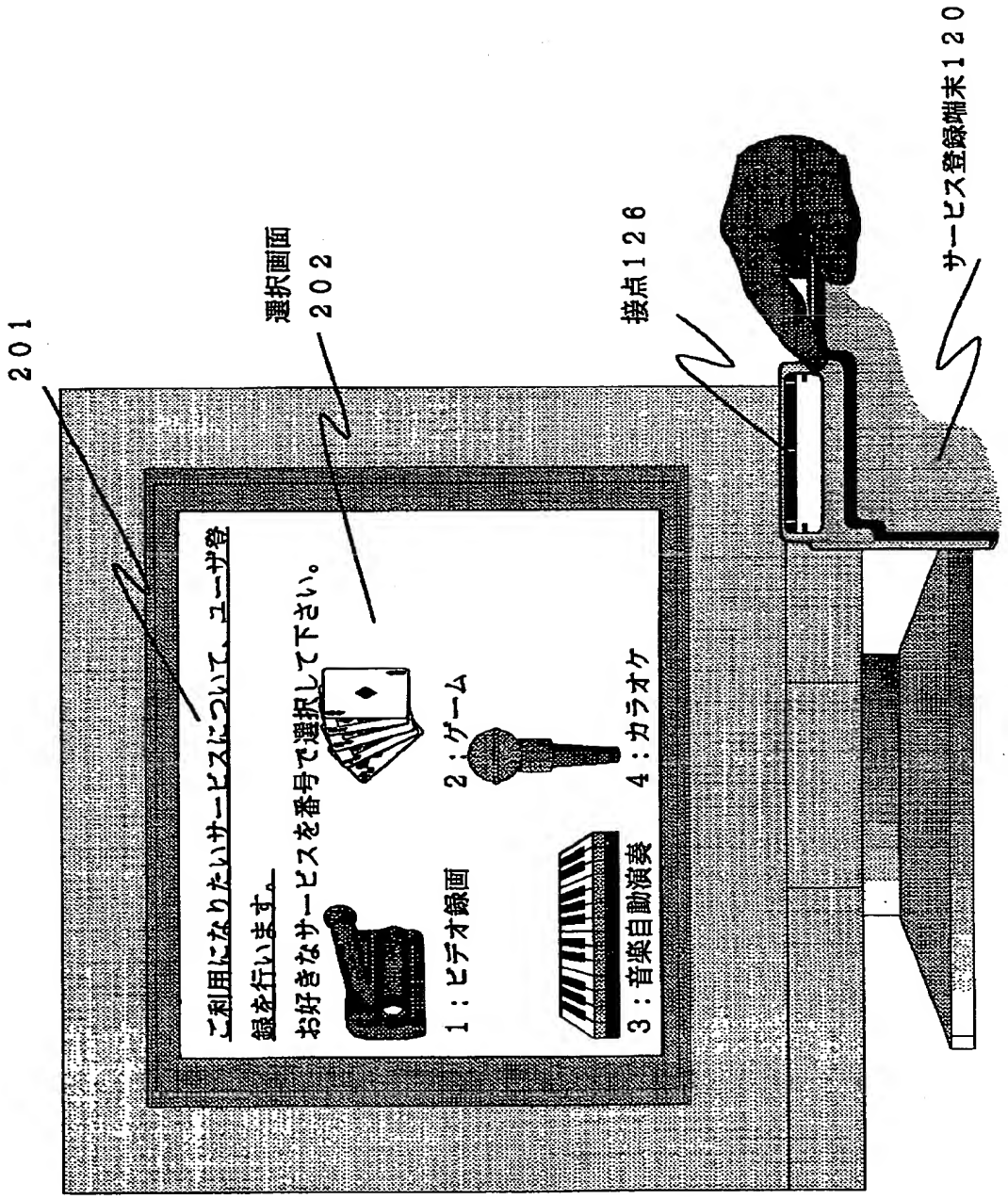
【図１１】



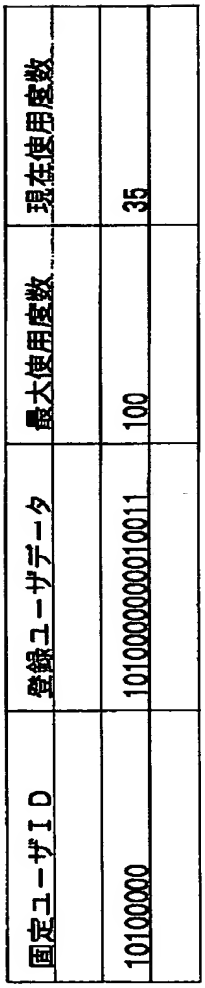
【図１２】


１１８
１１９
ユーザ３０
１１１
１１２
１１３
CPU
ROM
RAM
接触／
非接触
通信部２
１１５
１１６
サービス識別子
記憶部
１１７
通信部１
１１４
携帯機器１００
１４０
サービス提供端末１１０
１２４
１３４
１２１
通信部１
１２３
１３１
通信部１
１３３
CPU
ROM
RAM
CPU
ROM
RAM
１２２
１３２
１３５
通信部２
ユーザ
識別子
生成部
サービ
ス選択
部
認証部
１２５
１２６
１２７
課金認証データ記憶部
１３６
サービス登録端末１２０
クリアリングハウス１３０
１２８

【図１３】

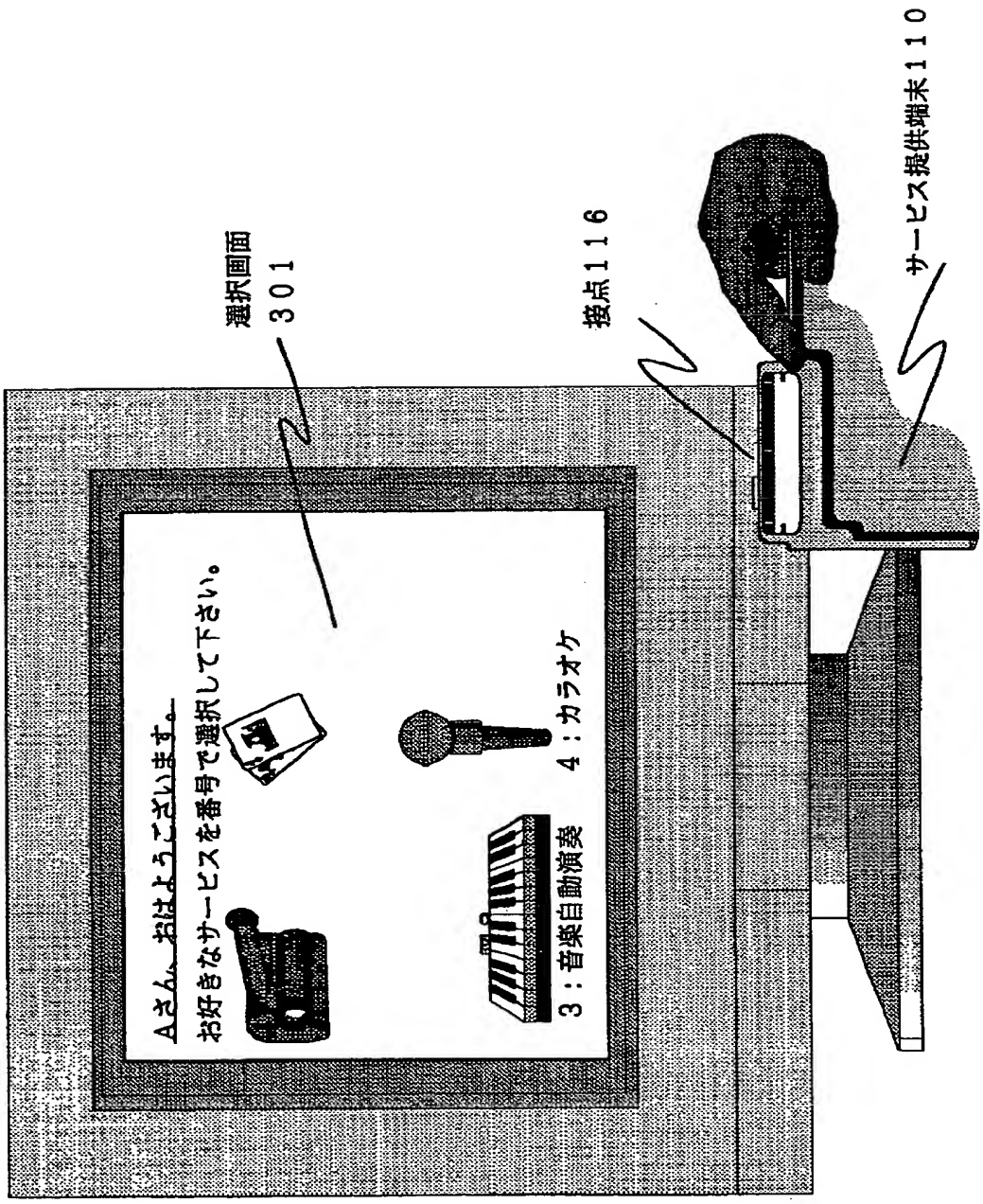

２０１
選択画面
２０２
接点１２６
サービス登録端末１２０
ご利用になりたいサービスについて、ユーザ登
録を行います。
お好きなサービスを番号で選択して下さい。
１：ビデオ録画
２：ゲーム
３：音楽自動演奏
４：カラオケ

【図１４】

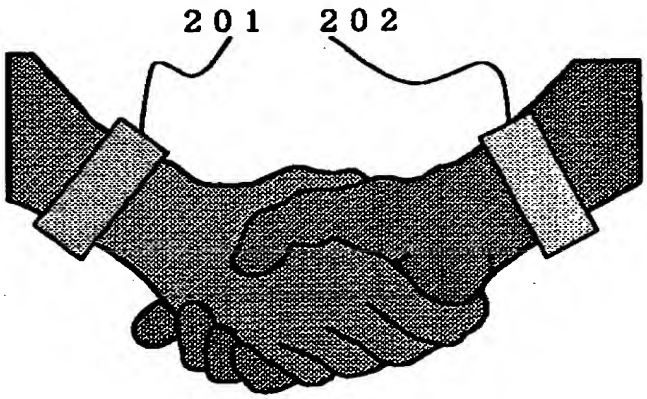


| 固定ユーザＩＤ | 登録ユーザデータ | 最大使用度数 | 現在使用度数 |
|---|---|---|---|
| 10100000 | 10100000000010011 | 100 | 35 |

【図１５】


選択画面
３０１
接点１１６
サービス提供端末１１０
Aさん、おはようございます。
お好きなサービスを番号で選択して下さい。
３：音楽自動演奏
４：カラオケ

【図１６】



【書類名】　要約書

【要約】

【課題】　人体を介した通信による個人認証処理実行システムにおいて、提供サービスに応じた認証を効率的に実行するシステムを提供する。

【解決手段】　ユーザが装着した携帯機器とサービス提供端末間での認証処理をサービス提供端末の接点に人体が触れることで実行する。ユーザの接触という物理的実感をともなって処理が行なわれる。さらに、ユーザの機器にユーザ固有識別子と、サービス端末の提供するサービスに応じて各ユーザごとに生成されるユーザ可変識別子とを格納し、サービス端末から送信されるサービス識別子に応じて、携帯端末で少なくともユーザ可変識別子に基づくサービス固有ユーザ識別データを生成してサービス端末に送付する構成とし、サービス内容に応じたユーザ単位の課金処理等、様々なユーザ管理を実行する。

【選択図】　図１

# 出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社